جرائم الحاسب الآلي
دراسة تحليلية

دكتور
أسامة حسين محى الدين عبد العال

تقديم عام

يصف العديد من رجال الإقتصاد والإجتماع والقانون الثورة الحالية للمجتمعات الصناعية بأنها ثورة المجتمعات المعلوماتيه، وهى ثورة صناعية ثانية مقارنة بالثورة الصناعية الأولى التى تحققت إبان القرنين التاسع عشر والعشرين الماضيين.

ويمكن القول بأنه إذا كان هدف الثورة الصناعية الأولى هو إحلال الآلة محل الجهد البدنى للإنسان، فإن هدف الثورة الصناعية الثانية هو إحلال الآلة (الحاسب الآلى) محل النشاط الذهنى للإنسان.

ومن الجدير بالذكر أن مجالات عديدة كالصناعة والتجارة والنقل والطب والتعليم والإتصالات والبحوث وغير ذلك الكثير والكثير ما كانت تتقدم وتتطور وتصل إلى هذه الكفاءة التى عليها الآن لولا عاملى السرعة والدقة اللذين توفرهما الحاسبات الآلية، بحيث أصبح من الصعوبة بمكان أن تقوم القطاعات المختلفة بأعمالها دون الإعتماد على الحاسبات الآلية....

ومع إزدياد الحاجة والعمل بالحاسب الآلى والنتائج الإيجابية المحققة نتطرق إلى الجانب السلبى لهذا الوضع وهو نشوء جرائم ناتجة عن ذلك الاستخدام، وهذه الجرائم إما أن تقع على الحاسب الآلى ذاته، وأما أن تقع بواسطته، بحيث يعد الحاسب الآلى أداة فى يد الجانى يستخدمه لتحقيق أغراضه الإجرامية.

ولما كانت جرائم الحاسبات الآلية أو كما يطلق عليها الفقة جرائم المعلوماتية لإرتباطها بالمعلومات المبرمجة آلياً هى ظاهرة حديثة النشأة لإرتباطها بتكنولوجيا حديثة هى تكنولوجيا الحاسبات الآلية، ولنا أن نتصور أن الكثيرين يروق لهم القول بأن الجريمة المعلوماتية هى أشبه بالخرافة، ولا تهديد حقيقى منبعة الحاسبات الآلية ، وأن كافة أشكال السلوك غير المشروع التى قد ترتبط بالحاسبات الآلية هى فى حقيقتها جرائم عادية يمكن بشأنها تطبيق النصوص الجنائية القائمة دونما أن تتميز بأية سمات خاصة.

وقد أسفرت محاولات التطبيق للنصوص التقليدية على هذا النوع الجديد

من الإجرام عن كثير من المشكلات القانونية، وإختلفت آراء الفقهاء فى شأن تطبيق النصوص القائمة عليها وتضاربت أحكام القضاء فى البلد الواحد، فصدرت أحكام تطبق النصوص القائمة على أى سلوك ينطوى على إعتداء على المعلومات المخزنة فى الحاسبات الآلية أو استعمالها غير المشروع، فى حين إعتبرته أحكام أخرى فعلاً مباحاً لم يرد بشأنه نص يجرمه ، بينما رأى البعض الأخر أن تلك النصوص ينحسر نطاق تطبيقها على الإحاطة بجرائم الحاسب الآلى لأن موضوعها يكمن فى المعلومات التى لا يمكن إعتبارها مالاً منقولاً لا تنسحب إليه الحماية الجنائية بمقتضى تلك النصوص[1].

أهمية دراسة جرائم الحاسب الآلى:

تتجلى أهمية دراسة جرائم الحاسب الآلى فيما يلى:

أولا: منذ الحالة الأولى الموثقة عام ١٩٥٨م لجريمة أرتكبت بواسطة الحاسب الآلى[2] وحتى الآن كبر حجم هذه الجرائم وتنوع أساليبها وتعددت إتجاهاتها وزادت خسائرها وأخطارها، حتى صارت من مصادر التهديد البالغة للأمن القومى للدول خاصة تلك التى ترتكز مصالحها الحيوية على المعلوماتية، وتحولت هذه الجرائم من مجرد إنتهاكات فردية لأمن النظم والمعلومات إلى ظاهرة تقنية عامة ينخرط فيها الكثير ممن تتوافر لديهم المهارة والمعرفة فى مجال الحاسبات ويرجع هذا التحول إلى عدة عوامل منها:

١- تزايد وعى المجرمين بإرتفاع عائد جريمة الحاسب الآلى وتدنى مخاطرها إذا ما قورنت بأية جريمة أو نشاط إجرامى آخر.

٢- إحباط وإستياء أفراد الطبقة المتوسطة فى المجتمع من الأوضاع والضغوط الإقتصادية المهيئ لإستغلال مراكزهم الوظيفية فى إدارة وتشغيل الحاسب لإرتكاب الجرائم بإستخدامه.

---

[1]- أنظر: د/ نائلة محمد فريد – جرائم الحاسب الإقتصادية (دراسة نظرية وتطبيقية) دار النهضة العربية- القاهرة ، ٢٠٠٤، صفحة ١١.

[2]- أنظر: د/ هشام محمد فريد رستم- قانون العقوبات ومخاطر تقنية المعلومات مكتبة الآلات الحديثة- أسيوط ١٩٩٤ هامش (١) صفحة ٩.

٣- إتساع دائرة إنتشار المعرفة بعلوم وتقنيات الحاسب والإقبال الهائل على تعلمها من قطاعات عدة فى المجتمع وحرص الكثير من الدول على تعليمها فى المدارس والجامعات.

٤- تركيز المعلومات المجسدة للأصول والأموال داخل الحاسبات .

٥- عدم كفاية رد فعل نظام العدالة الجنائية لمواجهة صور الإجرام المعلوماتى والذى يتجلى بشكل بالغ الدلالة فى إنخفاض فرصة تعرض مرتكبيها للإيداع فى المؤسسات العقابية بعد إدانتهم قضائياً.

٦- صعوبة إثبات هذه الجرائم نظراً لخبرة ومهارة ومعرفة الجناة العالية بثغرات القوانين الجنائية من ناحية، ولعدم كفاية النصوص الجنائية القائمة فى أغلب دول العالم على تحقيق أدوارها العقابية فى مكافحة هذا النوع من الإجرام المنظم، إما لقصور قاعدة التجريم عن تغطية معظم صور الإجرام المعلوماتى، أو لإعتمادها على وسائل الإثبات التقليدية التى تؤدى إلى إفلات كثير من الجناة فى تلك الجرائم عن العقوبات التى تقررها هذه القواعد الجنائية إضافة لذلك إرتكاب صور عديدة من الجرائم المعلوماتية على إقليم أكثر من دولة، بما يصعب جهود فرق البحث الجنائى من إكتشاف الجناة وتعقبهم وإنزال العقوبات الجنائية الملائمة عليهم إن وجدت.

ثانيا: أدى ظهور هذه الأنواع من الجرائم المعلوماتية إلى تبلور أنماط جديدة من الإعتداءات على الحقوق والمصالح التقليدية بتكنيك معلوماتى جديد، ولعل من أهم صور هذه الإعتداءات (غش الكمبيوتر) إختراق شبكة المعلومات، تزييف النقود بوسائل إلكترونية ، تزوير المستندات الإلكترونية والإعتداء على الملكية المعلوماتية، إتلاف البرمجيات وتدميرها وسرقة المعلومات وغسيل الأموال عبر الإنترنت، وغير ذلك من صور الإجرام المعلوماتى التى يصعب حصرها، فضلاً عن إستخدام تقنية المعلومات الحديثة فى إرتكاب الجرائم التقليدية ، كعمليات التجسس وسرقة الأموال التقليدية بتكنيك معلوماتى جديد، وعمليات الإغتيال والتفجير للأشخاص والأماكن باستخدام الكمبيوتر وتقنية الإتصال عن بعد، والسب والقذف وإنتهاك الآداب والأخلاق عبر شبكات

الإتصالات المتشعبة وشبكات الإنترنت[٣].

ثالثا: أصبحت الحياة الخاصة للأفراد التى تعتمد فى الكثير من مظاهرها على تقنية المعلومات المستخدمة، مجالاً لصور متعددة للإنتهاك، كتجميع المعلومات الإسمية عن طريق بنوك المعلومات كما أصبحت حقوق الملكية الفكرية فى مجال تقنية المعلومات مجالا خصباً للسرقة والسلب.

رابعا: أدى ظهور الإنترنت وسهولة إستخدامه إلى تغير فى شخصية ومواصفات من يرتكب جرائم الحاسب الآلى، وبصفة خاصة جرائم الإنترنت ، فإذا كانت جرائم الحاسب الآلى قد أرتكبت فى الماضى من أشخاص على قدر كبير من الذكاء حيث كان لا يصل إلى جهاز الكمبيوتر سوى المبرمج أو المستخدم المؤهل، فإن تطور الحاسبات الآلية وظهور الكمبيوتر الشخصى وسهولة استخدامه والتعامل مع الإنترنت ، قد قام بتوسيع نطاق وحجم المتعاملين مع الحاسب الآلى وشبكة الإتصالات المعلوماتية المتشعبة، وترتب على أن أصبح من الصعوبة بمكان حصر من يرتكبون جرائم الإنترنت فى طبقة أو فئة أو جنس معين، فمرتكب الجريمة المعلوماتية قد يكون من البالغين أو من الأحداث أو المتعلمين والمثقفين ومن الفقراء أو الأغنياء، كما لم يعد بالإمكان حصر جرائم الإنترنت فى نوع معين من الجرائم، فقد تكون من الجرائم الماسة بأمن الدولة من جهة الداخل أو الخارج، وقد تكون من جرائم الإعتداء على الأشخاص أو الأموال.

ومما تقدم يتبين لنا بوضوح مدى أهمية دراسة جرائم الحاسب الآلى أو جرائم المعلوماتية، التى أصبحت ظاهرة تستحق التركيز عليها ووضعها داخل دائرة الضوء وبؤرة إهتمام الباحثين.

٣- انظر: د/ سعيد عبد اللطيف حسن – إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت – (الجرائم الواقعة فى مجال تكنولوجيا المعلومات) – دار النهضة العربية- القاهرة- الطبعة الأولى – ١٩٩٩ صفحة (٧).

صعوبة الدراسة:

لاشك أن تطور الحاسب الآلى المذهل والسريع وظهور الإنترنت وإزدهار الحاسبات الآلية ، والإقبال الكبير على إقتنائها، أدى ذلك إلى إزدياد حجم المتعاملين فى مجال الحاسب الآلى ، واستتبع أيضا أن أصبح من الصعوبة حصر من يرتكبون الجرائم المعلوماتية، وكذا حصر نوعيات هذه الجرائم.

هذا من ناحية ومن جانب آخر الأمر يتعلق بإثبات الجرائم المعلوماتية فمن الجدير بالذكر أن المشكلة الرئيسية فى مجال إثبات جرائم الحاسب الآلى والإنترنت صعوبة إكتشافها وعند إكتشافها يصعب ملاحقتها لأسباب منها ذكاء ودهاء مرتكبيها والسرعة الفائقة فى إرتكاب هذه النوعية من الجرائم والإجرام المنظم.

وقد ترتب على ذلك أن الأدلة التقليدية فى الإثبات أصبحت غير مناسبة لإثبات الجرائم المعلوماتية، الأمر الذى يستلزم البحث عن أدلة جديدة من ذات الحاسب الآلى، ومن هنا تبدأ صعوبات البحث عن الدليل وتجميعه ومدى مصداقيته وقبوله فى إثبات وقائع هذه الجرائم[٤].

وأمام هذا الشكل الجديد من أشكال الإجرام، لا يبدو القانون الجنائى الحالى كافياً لكبح جماح هذا النوع الجديد من الإجرام المنظم، فنصوص التجريم التقليدية قد وضعت فى ظل تفكير يقتصر إدراكة على الثورة الملموسة والمستندات ذات الطبيعة المادية، مما يتعذر معه تطبيقها لحماية القيم غير المادية المتولدة عن المعلوماتية[٥].

إختيار موضوع الدراسة:

سبق القول أن مجالات عديدة كالصناعة والتجارة والإقتصاد والتعليم

---

[٤]- انظر: د/ سعيد عبد اللطيف حسن – إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت – (الجرائم الواقعة فى مجال تكنولوجيا المعلومات) – دار النهضة العربية- القاهرة- الطبعة الأولى – ١٩٩٩ صفحة (٩).

[٥]- أنظر: د/ هشام محمد فريد رستم- قانون العقوبات ومخاطر تقنية المعلومات مكتبة الآلات الحديثة- أسيوط ١٩٩٤ - صفحة ١١، ١٢ .

والطب والهندسة، وغير ذلك ما كانت تتقدم بذات الكفاءة التى هى عليه الآن، ويعزى ذلك بعاملى السرعة والدقة اللذين توفرهما الحاسبات الآلية ، ويمكن القول بأنه من الصعب الآن أن يقوم قطاع معين بأعماله دون الإعتماد على الحاسبات الآلية.

وقد أدى ذلك إلى نشوء جرائم ناتجه عن ذلك الاستخدام، ولما كانت هذة الجرائم لم نعهدها من قبل، فإن تطبيق النصوص الجنائية القائمة عليها يسفر عن كثير من المشكلات القانونية، خاصة وأن مجرمى هذا النوع يتميز بالذكاء والوعى الشديدين، إضافة إلى صعوبة إثبات هذه الجريمة.

وإنطلاقاً مما تقدم، وعلى الرغم من أن المراجع والمؤلفات والدراسات فى هذا النوع من الإجرام لا تتطور ولا تتناسب مع إزدياد وتطور هذه الجرائم ، وبالتالى يصبح البحث والتحرى واستسقاء المعلومة المؤكدة من الصعوبة بمكان، ومع كل هذه الإعتبارات فقد رأينا البحث فيه محاولة منا لإلقاء بعض الضوء، كمحاولة جادة للتوصل إلى أوصاف دقيقة لمفهوم الجريمة المعلوماتية، والمجرم فى هذه الجريمة، إنطلاقاً من البحث فى مفهومه وقواعده، مع التعمق فى البحث والتوثيق التاريخى لتشريعات الكمبيوتر.

منهج الدراسة:

حتى تؤتى هذه الدراسة ثمارها المرجوة، سنعمل بعون الله وتوفيقه على إتباع المنهج التحليلى والتاريخى لتشريعات الكمبيوتر.

أ- المنهج التاريخى:

يعطى هذا المنهج أهمية كبيرة لنشاة النظام القانونى وتطوره فى السنوات السابقة، الأمر الذى يساعدنا على تشخيص الظاهرة، مما نأمل معه التوصل إلى حلول مناسبة تتناسب مع الفكر والظروف الحالية.

ب- المنهج التحليلى:

ويتم ذلك باستعمال التحليل المنطقى لتشريعات الكمبيوتر والجرائم المتعلقة به، بغية إستخلاص حكم المسائل التى يثور حولها الغموض والإختلاف.

خطة الدراسة:

إحقاقاً للحق، لا أدعى قط أن هذه الدراسة قد ألمت بكل جوانب جرائم الحاسب الآلى، أوغطت جانباً متكاملاً له، فذلك عمل ليس باليسير ولا تتسع له صفحات الدراسة، إنما هو عمل موسوعى نظراً لتطور وتعدد مجالات الدراسة.

وفى الواقع حاولت أن أستنتج معالم جد موجزة عن هذه الجرائم، لذلك فالدراسة تقوم على ثلاثة فصول تحليلاً وتوضيحاً للصورة وقد مهدت للموضوع بمقدمة عامة تناولت فيها أهمية دراسة هذا النوع من الإجرام وصعوبة البحث فيه وأسباب إختيار هذه الدراسة ومنهجها.

وقد قسمت الدراسة على النحو التالى:

الفصل الأول: التأصيل التاريخى لتشريعات جرائم الكمبيوتر.

الفصل الثانى: مدلول الجريمة المعلوماتية.

الفصل الثالث: تقسيم الجرائم المعلوماتية.

الخاتمة والتوصيات.

الفصل الأول
التأصيل التاريخى لتشريعات جرائم الكمبيوتر

تمهيد:

إن ظاهرة جرائم الكمبيوتر والإنترنت أو جرائم التقنية العالية، أو الجريمة الإلكترونية، أو السيبر كرايم (Cyber crime) ، ظاهرة إجرامية حديثة نسبياً تقرع فى جنباتها أجراس الخطر لتنذر مجتمعات العصر الراهن لحجم المخاطر وهول الخسائر الناجمة، بإعتبارها تستهدف الإعتداء على المعطيات بدلالتها التقنية الواسعة (بيانات ومعلومات وبرامج بأنواعها).

وبالتالى فهى جريمة تقنية تنشأ فى الخفاء يقارفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية ، توجه للنيل من الحق فى المعلومات وتطال إعتداءاتها معطيات الكمبيوتر المخزنة، والمعلومات المنقولة عبر نظم وشبكات المعلومات وفى مقدمتها الإنترنت .

هذه المعطيات هى موضوع هذه الجريمة ، وما تستهدفة إعتداءات الجناة تظهر مدى خطورة جرائم الكمبيوتر، فهى تنال الحق فى المعلومات، وتمس الحياة الخاصة للأفراد وتهدد الأمن القومى والسيادة الوطنية، وتشيع فقدان الثقة بالتقنية وتهدد إبداع العقل البشرى.

لذا فإن ادراك ماهية جرائم الكمبيوتر والإنترنت والطبيعة الموضوعية لهذه الجرائم، وإستظهار موضوعها وخصائصها ومخاطرها وحجم الخسائر الناجم منها وسمات مرتكبيها ودوافعهم ، يتخذ أهمية إستثنائية لسلامة التعامل مع هذه الظاهرة ونطاق مخاطرها الاقتصادية والأمنية والاجتماعية والثقافية.

وإنطلاقاً من ذلك ، فقد تزايدت خطط مكافحة هذه الجرائم، وانصبت الجهود على دراستها المتعمقة، وخلق آليات قانونية للحماية من أخطارها، وبرز فى هذا المجال المنظمات الدولية والإقليمية ، خاصة المنظمات والهيئات الاقليمية الأوروبية، وإدراكاً لقصور القوانين الجنائية بما تتضمنه من نصوص التجريم التقليدية، كان لابد للعديد من الدول وضع قوانين وتشريعات خاصة لضمان توفير الحماية القانونية الفاعلة ضد هذه الجرائم[٦].

[٦]- إن مواجهة هذه الجرائم تم فى ثلاثة قطاعات مستقلة (حماية الكمبيوتر أو ما يعرف بجرائم

ويعد من أكثر مسائل ظاهرة جرائم الكمبيوتر والإنترنت إثارة للجدل والنقاش إلى جانب تعريفها وتحديد موضوعها أو مناط الحماية ومحله مسألة تحديد قائمة جرائم الكمبيوتر وتحديد انماط السلوك الإجرامى والافعال المكونه له وبيان التركيب القانونى لهذه الجرائم، وهذه المسائل اجتمعت الآراء فيها نحو عدم قابلية النصوص الجنائية التقليدية عن مواجهتها وعدم كفايتها للإنطباق على هذه الانماط الجديدة من الجرائم نظراً للتطور السريع فى هذه النوعية من الجرائم.

وهذا يستدعى دون أدنى شك تعديل قوانين العقوبات الوضعية وتبنى قوانين جديدة، بحيث لا تبقى بعض أو كل جرائم الحاسب الآلى خارج نطاق النص التشريعى وبالتالى بمنأى عن العقوبة[٧].

وانطلاقاً مما تقدم فإننا سنتناول هذا الفصل فى مبحثين على النحو التالى:

المبحث الأول : التأصيل التاريخى لتشريعات جرائم الحاسب الآلى

المبحث الثانى : مفهوم قانون الكمبيوتر

الكمبيوتر ذات المحتوى الاقتصادى، وحماية البيانات المتصلة بالحياة الخاصة (الخصوصية المعلوماتية) وحماية حق المؤلف على البرامج وقواعد البيانات (الملكية الفكرية للمصنفات الرقمية)– انظر عبر الإنترنت Lawoffc@nol.com.jo

[٧]- فى ذلك يقول الفقية الالمانى (Ulrich sieber) " لقد اظهر التحليل للقوانين المختلفة ان الحماية الجنائية للمعلومات فى كل دولة بحاجة ماسة لوضع نظرية عامة لها ومرد ذلك انه فى غالب الحالات تمت مناقشة الحماية الجنائية لكل من الحياة الخاصة والأموال والحقوق الذهنية إزاء إجرام تقنية المعلومات على حدة" ويعد هذا الفقية الألمانى أشهر القانونيين فى ميدان دراسات جرائم الكمبيوتر، وله العديد من المؤلفات منذ منتصف السبعينات، وقد كلف عام ١٩٩٨ من قبل اللجنة الأوروبية ومجلس أوروبا لوضع دراسة تفصيلية تحليلية بخصوص الموقف القانونى والتشريعى لدول إتحاد أوروبا جميعاً مقارنة بامريكا وكندا واستراليا حول جرائم الكمبيوتر تعد الأوسع والأشمل فى هذا المجال – انظر :

Ulrich sieber (legal aspects of computer – related crimes, eu comcrime, 1998).

المبحث الأول
التأصيل التاريخى لتشريعات جرائم الحاسب الآلى

إن كل اختراع أو فتح علمى يفرز واقعاً جديدا ويرتب آثاراً ما كانت قائمة قبل وجود وشيوعه، فاختراع الطائرة مثلاً خلق آثاراً جديدة فى مجال نقل الأفراد والبضائع، فالطائرة تجوب العديد من الدول أثناء ترحالها فى الفضاء الجوى الذى يعلو هذه الدول، والطائرة قد تكون وراء ضرر يلحق بالركاب على متنها وقد يتعرض سطح الأرض وما عليه من أملاك واشخاص للخطر.

والطائرة وسيلة نقل هامة تتطلب أموالا هائلة للاستثمار وتتطلب ان تلحقها خدمات عديدة غير متصلة بالطائرة ذاتها وانما تتعلق بخدمات المسافرين والمطارات وخدمات الفضاء الجوى، وهذة الوسيلة بما تملكه من قدرات التنقل والاختراق قد تعرض امن الدولة للخطر، ولضمان سلامة الطيران ورعاية قواعده وتوحيدها نشأت الهيئات والمنظمات الدولية والاقليمية والمتخصصة فى مجال الطيران.

هذه الأثار وغيرها افرزها هذا الاختراع العلمى المميز، وتطلب التعامل معها حزمة من التشريعات الوطنية والاتفاقيات الدولية والاقليمية والثنائية، عالجت وتعالج النظام القانونى للطائرة والمطارات وخدمات الركاب والشحن وما ينشأ فى بيئتها من علاقات قانونية وتعالج المسئولية عن الاضرار اللاحقة بالركاب وبالأشخاص والممتلكات على سطح الارض وغيرها العديد من المسائل فيما أصبح يعرف بالقانون الجوى.

وبايجاز فالطائرة خلقت فرعا جديداً من فروع القانون تتكامل فيه النظريات والقواعد وتمتد من النطاق الوطنى إلى النطاقين الاقليمى والدولى، وذات الامر يقال بشأن العديد من المخترعات والإكتشافات.

وبذات المنطق افرزت تقنية المعلومات آثاراً شاملة على البناء الإدارى والإقتصادى والسياسى والاجتماعى والثقافى والقانونى للدولة وقد أثرت على مختلف مناحى النشاط الانسانى.

ومما هو ثابت أن القراءة التاريخية التحليلية لحركة التشريع فى مجال قانونى معين تقدم أساساً هاماً لتحقيق رؤية شاملة فى التعامل مع هذا المجال ، مسائلة وتحدياته وبدونها قد لا يتحقق الإنسجام والتناغم فى الحلول والتدابير التشريعية التى تستهدف تنظيم هذا المجال ، وجدير بالذكر أن التعامل مع تشريعات تقنية المعلومات حتى فى أكثر الدول تقدماً جاءت قاصرة عن الاحاطة الشاملة بالمتطلبات التشريعية والقانونية لهذا المجال، ويلاحظ ان التعامل مع تقنية المعلومات تشريعياً تم خلال حقب زمنية متباينة وتناول قطاعات وموضوعات دون غيرها.

ففى ميدان جرائم الكمبيوتر مثلا، تم التعامل مع الحماية الجنائية للمعلومات ضمن ثلاث محاور منفصلة:

أولها: - حماية البيانات الشخصية المخزنة فى نظم المعلومات من مخاطر المعالجة الالية، وهو ما يقع ضمن دراسات حقوق الإنسان باعتباره ينصب على حماية الحق فى الخصوصية Privacy، أو الحياة الخاصة.

وثانيها: حماية المعلومات ذات القيمة المالية أو التى تمثل اصولا مالية من مخاطر الانماط الجرمية المستجدة التى تعتمد الكمبيوتر وسيلة للجريمة أو هدفا أو بيئة لها، وهو ما عرف ايضا بجرائم الكمبيوتر Computer crimes أو الجرائم المرتبطة بالكمبيوتر Computer- Related Crimes أو جرائم الكمبيوتر ذات الطبيعة الاقتصادية Economic Computer Crimes أو غير ذلك من اصطلاحات دالة عليها، ويقع ضمن نطاق دراسات القانون الجنائى الموضوعى وهو ما عبر عنه بالعموم بوصفه الحق فى المعلومات .

وثالثها: حماية برامج الحاسبات من مخاطر القرصنة المتمثلة بالنسخ غير المصرح به واعادة الانتاج والتقليد وهو ما يقع ضمن دراسات الملكية الفكرية وتحديداً حقل حماية حق المؤلف Copyright.

والحق أن محاولة تقصى التدابير التشريعية فى حقل تقنية المعلومات يعنى العودة إلى بداية السبعينات.

فالتطور التاريخى لتقنية المعلومات، يشير إلى ان السبعينات تحديدا شهدت إنتقالا حقيقيا فى ميدان استخدام الحوسبة وتقاربها بانظمة الاتصالات، فالسبعينات شهدت التوجه نحو بناء الحواسيب الشخصية وشهدت إتساعا تجارياً

حقيقياً فى إستخدام الحوسبة، وشهدت إنجازات فى حقل تشبيك الحواسيب وربطها مهدت لولادة عصر الشبكات. وبالرغم من أن العديد من المسائل المتصلة بإستخدام الكمبيوتر قد أثيرت منذ الخمسينات والستينات إلا أن تلك المعالجات لم تؤد إلى اتخاذ تدابير تشريعية، لتكون ولادة القوانين الحقيقية ذات الصلة بالكمبيوتر قد تحققت مع مطلع السبعينات.

إن المرور بمنحنيات الزمان والمكان والموضوع، سيحملنا ضمن منحنيات متداخلة، إذ يتحقق التداخل بين الفترات الزمنية لكل طائفة من التشريعات، كما يتحقق التداخل بالنسبة للموضوعات محل التنظيم، ودون القفز إلى النتائج فى هذا المقام، فإننا سنعمد إلى تقصى المسيرة التاريخية لتشريعات تقنية المعلومات، من خلال تتبع موجات التشريع وتحديد اطارها العام.

ويمكننا القول بأن الملامح الأولى لقانون الكمبيوتر بدأ مع شيوع استعمال الكمبيوتر، ولأنه أداة جمع ومعالجة للمعلومات فقد كانت أول تحدياته القانونية إساءة الاستخدام على نحو يضر بمصالح الأفراد والمؤسسات، ومعه نشأ الإرتباط بين القانون والكمبيوتر الذى إنطلق من التساؤل فيما إذا كانت أنشطة إساءة إستخدام الكمبيوتر تقييم مسئولية قانونية أم أنها مجرد فعل غير مرغوب فيه أخلافيا ؟ً

وماذا إذا كان يتعين تنظيم استخدام الكمبيوتر أم لا؟

وهذا التساؤل اثير فى مجالين : الأول : - المسئولية عن المساس بالأفراد والمؤسسات عند إساءة التعامل مع بياناتهم الشخصية المخزنة فى نظم الكمبيوتر على نحو يمس أسرارهم حقهم فى الخصوصية، والثانى: المسئولية عن الأفعال التى تمس أو تعتدى على أموال الأفراد ومصالحهم وعلى حقهم فى المعلومات ذات القيمة الاقتصادية ، ولو دققنافى هذين المجالين لوجدنا أنفسنا أمام (الخصوصية) و (جرائم الكمبيوتر).

إذن ثمة حقيقة أولى أن بداية قانون الكمبيوتر إرتبط بالبحث فى المسئولية عن أنشطة تتصل بالمعلومات ونظمها وتحديداً فى المجال الجزائى.

والجدل الذى دار فى ذلك الوقت (الستينات تحديداً وإمتد إلى مطلع السبعينات) أشبة بالجدل الدائر منذ نحو خمس سنوات بشأن الإنترنت: هل يتعين إخضاع التقنية الجديدة، توظيفها وإستخدامها- للتنظيم القانونى ام تترك للتنظيم

الذاتى، أو كما يعبر عنه الفكر الرأسمالى (تنظيم السوق نفسه) فلا نكون أمام قواعد قانونية تقر من الاطر الحاكمة بل أمام قواعد سلوكية وشروط عقدية.

فى هذا الاطار فإن أول حالة موثقة لإساءة استخدام الكمبيوتر ترجع إلى عام ١٩٥٨ وفقا لما لنشرة معهد ستانفورد فى الولايات المتحدة الامريكية ، ليبقى الحديث من ذلك الوقت وحتى مطلع السبعينات فى إطار البعد الأخلاقى وقواعد السلوك المتعين أن تحكم استخدام الكمبيوتر ولتتجه الجهود والمواقف نحو حسم الجدل باعتبار اساءة استخدام الكمبيوتر فعلاً موجباً للمسئولية القانونية، ولتنطق التشريعات الوطنية فى مجال جرائم الكمبيوتر مع نهاية السبعينات (تحديداً فى الولايات المتحدة إبتداء من ١٩٧٨). أما الجهد الدولى فقد تحقق إبتداء فى مجال الخصوصية، ففى عام ١٩٦٨ ، شهد مؤتمر الأمم المتحدة لحقوق الإنسان طرح موضوع مخاطر التكنولوجيا على الحق فى الخصوصية، إذ بالرغم من أن الحق فى الخصوصية نشأ قبل هذا التاريخ حظى بجدل قانونى وقضائى وفكرى منذ مئات السنين، فإنه لم يكن ثمة إثارة لما يتصل بهذا الحق متعلقاً بالمعلومات الشخصية المعالجة آليا بالقدر الذى أثير فى المؤتمر المشار إليه، والذى استتبعه إصدار الامم المتحدة. قرارات فى هذا المجال لتشهد بداية السبعينات (تحديد عام ١٩٧٣ فى السويد) إنطلاق تشريعات قوانين حماية الخصوصية مع الإشارة إلى أنها نوقشت فى نظم قانونية أجنبية كثيرة- كدول أوروبا الغربية مثلا – ضمن مفهوم حماية البيانات **Data protection.**

وإنطلاقاً مما تقدم يمكننا القول بأن الخصوصية وحماية البيانات تمثل أول مجال من مجالات قانون الكمبيوتر من حيث الإهتمام التنظيمى الدولى ويعد ذلك بمثابة الحقيقية الثانية.

ولأن السبعينات بحق الإدراك العميق لأهمية برامج الكمبيوتر وباتت تشير إلى أنها ستكون القيمة الأكثر أهمية من بين عناصر تقنية المعلومات وستفوق عتاد الكمبيوتر المادى فى أهميتها ، فإن مطلع السبعينات شهد جدلاً واسعاً حول موقع حماية برامج الكمبيوتر، أهى قوانين براءات الاختراع بوصف البرنامج من المصنفات القابلة للاستثمار فى حقل صناعات الكمبيوتر؟ أم أنها تشريعات حق المؤلف باعتبار البرنامج فى الأساس ترتيبت منطقى لأوامر كتابية؟ هذا الجدل ربما لم يمنع من أن يتفق الجميع على وجوب الحماية، لكن

الخلاف كان فى موضعها، فإلى جانب هذين التوجيهين، كان ثمة آراء تجد فى القواعد القانونية المدنية والشروط العقدية (تحديدا فى حقل المنافسة والأسرار) موضعاً مناسباً لحماية حقوق المبرمجين. فى هذه البيئة الجدلية بدأت تظهر التدابير التشريعية فى حقل حماية البرمجيات إعتبارا من ١٩٧٣ (فى الفلبين) مع أن موجة هذه التشريعات يتم إرجاعها للثمانينات لأن الأخيرة شهدت تدابير تشريعية وطنية واسعة فى حقل حماية البرمجيات بسبب الأثر الذى تركته القواعد النموذجية لحماية برامج الكمبيوتر الموضوعة من خبراء المنظمة العالمية للملكية الفكرية (الوايبو) عام ١٩٧٨.

وصحيح أن تشريعات حماية البرامج ترافقت مع تشريعات الخصوصية وجرائم الكمبيوتر، لكنها كانت أسرع تنامياً وأوضح من حيث الرؤى للمحتوى ولمستقبل هذه التشريعات، ولهذا فانها أوسع مدى من حيث عددها وإذا أردنا أن نعرف السر فإنه فى الحقيقة يرجع إلى عاملين أساسيين ، الأول: وجود المنظمة العالمية للملكية الفكرية (الوايبو)، التى ساهمت عبر ملتقياتها وأدلتها الإرشادية وقوانينها النموذجية فى حسم الجدل بشأن موضع حماية البرمجيات ليكون قوانين حق المؤلف. والثانى:- التوجه الإستراتيجى للأسواق الرأسمالية للإستثمار فى حقل الملكية الفكرية ومصنفاتها كمقدمة لبناء الاقتصاد الرقمى الذى بدأت أول ملامحة فى إتجاه الولايات المتحدة الأمريكية مدفوعه بتأثير الشركات متعددة الجنسيات لوضع الملكية الفكرية ضمن أجندة إتفاقيات تحرير التجارة والخدمات ومساومة الولايات المتحدة العالم كله على قبول اتفاقيات تحرير التجارة فى البضائع مقابل إنجاز تقدم فى مجالى تحرير الخدمات والملكية الفكرية[٨].

[٨]- كانت الولايات المتحدة الامريكية من بين الدول التى رفضت الانضمام لإتفاقيات الجات (١٩٤٧) المتعلقة بتحرير التجارة فى البضائع . وظل موقفها هذا واضحا فى جولات المفاوضات التجارية السبعة حتى بدات جولة الاورغواى (١٩٨٦-١٩٩٤) والتى شهدت تحولاً رئيسياً فى التجارة الدولية عنوانه قبول امريكا ضمن تحالف مصالح مع عدد من الدول الصناعية اتفاقيات عديدة فى حقل تحرير تجارة البضائع مقابل ادراج اتفاقيات تحرير الخدمات (جاتس) واتفاقية الملكية الفكرية هذا التحول الذى ادى إلى ولادة منظمة التجارة اعتبارا من ١٩٩٥/١/١ بموجب اعلان مراكش انظر تفصيلا (الكتاب الخامس من موسوعة القانونية وتقنية المعلومات) دليل التجارة الدولية والاستثمار (اتفاقيات

ولا يعنى هذا أن بقية موضوعات تقنية المعلومات لم تحظ بدعم وإهتمام هيئات دولية، لكن الفرق أن أيا منها حتى ذلك الوقت لم يكن موضع عمل منظمة متخصصة فيه كما هو حال منظمة الوايبو التى تتولى رعاية الملكية الفكرية وإدارة اتفاقياتها.

إذن الحقيقة الثالثة، أن أكثر تشريعات قانون الكمبيوتر نضجاً ووضوحاً فى أغراضها القوانين أو التدابير التشريعية المتعلقة بحماية الملكية الفكرية لبرامج الكمبيوتر (وفيما بعد قواعد البيانات والدوائر المتكاملة) ويتصور أن تحقق هذه التشريعات أيضا حماية أوسع فى السنوات القادمة فى مجال أسماء مواقع الإنترنت والمحتوى الرقمى لمواقع الإنترنت.

وقبل أن نتواصل مع حقائق التاريخ، علينا أن نصل فى هذا المقام إلى استنتاج ، أن مطلع السبعينات شهد الإنطلاقة الحقيقية لحزمة تشريعات الخصوصية وأن السبعينات أيضاً (وعلى إمتداد الثمانينات والتسعينات) شهد إنطلاقة الحزمة الثانية المتمثلة بقوانين جرائم الكمبيوتر، فى حين شهدت الثمانينات (فعلياً) إنطلاقة حزمة ثالثة من التشريعات المتصلة بالكمبيوتر هى حزمة تشريعات حماية البرمجيات التى تمثل المصنف الأهم من بين المصنفات الرقمية ذات الاتصال بالكمبيوتر

ثلاثة حزم تشريعية: تشريعات الخصوصية (حمايةا لحق فى البيانات الشخصية من مخاطر التكنولوجيا) ، قوانين جرائم الكمبيوتر (الإعتداء على نظم المعلومات والمعلومات ببعدها الاقتصادى) وتشريعات حماية برامج الكمبيوتر (الملكية الفكرية).

هذه مجالات ثلاثة فى ساحة قانون الكمبيوتر، وسنجد أن ثمة مجال رابع يكاد يكون الوعاء الذى يضمها جميعاً وهو مجال الأعمال الالكترونية، لكن يفصل بين مجال الأعمال الالكترونية والمجالات الثلاثة، فروع أخرى ربما لا تكون مستقلة بشكل كاف فى مبناها عن الفروع القانونية التى تتبعها لكنها بالتأكيد خلقت تغيرات جوهرية إستلزمتها تقنية المعلومات. فأول الفروع التى برزت عقب الفروع الثلاثة المتقدمة، قواعد الإجراءات الجنائية للإستدلال والتحقيق والإثبات وإجراءات المحاكمة المتفقة مع طبيعة الإعتداءات فى الدعاوى التى

منظمة التجارة الدولية) عبر شبكة الإنترنت www.law-d7.com

تتعلق بجرائم الكمبيوتر أو الإعتداء على الخصوصية وحتى فى مجال قرصنة برمجيات الحاسوب المخزنة داخل النظم أو المحملة مع الأجهزة. وبالرغم من أن الدول الأوروبية وإستراليا كذلك قد تنبهت لهذا الموضوع مبكراً مع مطلع السبعينات إلا أن الحزمةالتشريعية المتصلة بهذه القواعد بدأت حقيقة وعلى نطاق واسع فى منتصف الثمانينات (إبتداء من عام ١٩٨٤ فى بريطانيا).

تبع هذا المجال تدابير تشريعية فى ثلاثة مجالات أخرى كان للإنترنت وشبكات المعلومات ونماء استثمارات الخدمات التقنية الدور فى توجيه الإهتمام الحقيقى بها، بل فى ولادة مفهوم جديد لبداياتها التى ظهرت قبل شيوع الإنترنت، فمع تحول الإنترنت إلى الاستخدام التجارى الواسع ، ظهرت تحديات قانونية جديدة، بعضها ذو إتصال بتحديات سابقة أو قائمة، كتحديات حماية أمن المعلومات فى مجالى الخصوصية وجرائم الكمبيوتر وحماية البرامج فى بيئة الإنترنت ذاتها، لما أتاحته من تسهيل إرتكاب الإعتداءات بعد أن وفرت مدخلاً سهلاً إلى نظم الكمبيوتر المرتبطة ضمنها، وتحديات أخرى أوجبتها أنماط السلوك الجدية التى ولدت بولادة الإنترنت، كالبيع والشراء على الشبكات وأداء الخدمة عبر الإنترنت، ومن هذه التحديات التنظيم القانونى للتجارة الإلكترونية.

هذه التحديات التى أوجدتها أو ضخمتها الإنترنت أو عدلت فى نطاقها ومخاطرها وجديتها، رافقها حزم تشريعية بدأت فى مجال ما يعرف بتنظيم الأمن المعلوماتى، والمعايير التقنية وتحديداً ما يتصل بتشفير البيانات ، التى إنطلقت فى عام ١٩٩٠ من فرنسا تحديدا، ثم فى مجال مكافحة المحتوى غير القانونى للمعلوماتية، الذى إنطلق عام ١٩٩٦ فى أمريكا. وأخيراً المجال الأكثر إثارة للجدل وأوسعها تنظيماً، مجال الأعمال الالكترونية الذى أشرنا أعلاه إلى أنه المجال الرابع المركزى إلى جانب جرائم الكمبيوتر والخصوصية والملكية الفكرية. ومجال الأعمال الالكترونى ليس لاحقا للمجالات الأخيرة الثلاث ، إنما قد نجد تشريعات فى إطارة كالتشريعات المتعلقة بتقنيات الأعمال المصرفية، أو تلك المتعلقة بحجية الاثبات بالوسائل الالكترونية، سابق بسنوات عديدة للمجالات المشار إليها، لكن قولنا بأنه المجال الأخير زمنيا يرجع إلى تبلور مفاهيم شمولية جديدة فى مجال الأعمال الإلكترونية عكسها تحديدا مفهوم التجارة الالكترونية والبنوك الإلكترونية وهذا المفهوم الشامل نجد أنه إنطلق مع عام ١٩٩٦ الذى

شهد إقرار القانون النموذجى للتجارة الإلكترونية من قبل لجنة الأمم المتحدة لقانون التجارة (اليونسترال). وسنجد أن دولاً على المستوى التشريعى كانت قد بدأت الأهتمام بمسائل الأعمال الإلكترونية (كالاثبات بالوسائل الإلكترونية وحجية مستخرجات الحاسبوت والتنظيم القانونى لبطاقات الائتمان وغيرها) من أواخر السبعينات وبداية الثمانينات ، لكنها لم تكن ضمن التصور الشامل للتجارة الإلكترونية التى إرتبطت واقعا بانشطة الاستثمار على الإنترنت .

أما من حيث الأطر الدولية العاملة فى ميادين الموضوعات المتقدمة ،فإننا سنجد الجهد الاساسى والمميز موزع بين منظمة التعاون الاقتصادى والتنمية وهيئات أوروبا- (مجلس أوروبا والمفوضية الاوربية واتحاد اوروبا والبرلمان الأوروبى) والأمم المتحدة، ومجموعة الدول الصناعية الثمانية والوايبو ، والانتريول ، ومنظمة التجارة الدولية وغيرها من المنظمات .

وإنطلاقا من ذلك يمكن القول بأن تشريعات قانون الكمبيوتر تنحصر فى: الخصوصية، جرائم الكمبيوتر ، الملكية الفكرية للمصنفات الرقمية، الإجراءات الجنائية فى البيئة الرقمية ، المعايير والمواصفات والأطر التنظيمية للتقنية وتأثيرها على النشاط الادارى والخدمى، المحتوى غير القانونى للمعلوماتية، الأعمال الإلكترونية وتحديداً التجارة الإلكترونية، وفى إطار كل منهما ثمة تشريعات ومجهودات دولية وإقليمية وسياسات وإستراتيجيات ومحتوى ومشكلات أيضا.

المبحث الثانى
مفهوم قانون الكمبيوتر

وفق التوصيف المتقدم أن المجالات التشريعية سبعة ، أربعة منها تكاد تستقل تماماً فى أطرها التنظيمية والتشريعية ، إلا أن كل منها شهد تطوراً فتفرع فى إطارها ايضا حقوق أخرى ، بعضها يرتبط بغيره وبعضها يستقل فى موضعه عنها، لكن حركة التطور- كما سيظهر من تحليل موضوعات هذه الحقول- يأخذها شيئا فشيئاً نحو التكاملية والتوحد فى إطار واحد ، وهذا ما سيؤدى إلى تبلور قانون الكمبيوتر كفرع مستقل عن بقية الفروع القانونية، ولو اعدنا حصر كافة القطاعات المتقدمة وما تفرع عنه سنجد انفسنا أمام المجالات التشريعية التالية فى نطاق قانون الكمبيوتر :

١- تشريعات الخصوصية أو قواعد حماية تجميع ومعالجة وتخزين وتبادل البيانات الشخصية.
٢- تشريعات جرائم الكمبيوتر ، ومن ثم تطورها لتشمل جرائم الإنترنت وشبكات الاتصال ضمن مفهوم اشمل (امن المعلومات).
٣- تشريعات الملكية الفكرية فى حقل حماية البرمجيات ومن ثم تطورها لتشمل بقية المصنفات الرقمية، إلى جانب تطورها على نحو يعكس الاتجاهات العالمية فى ادراج الملكية الفكرية ضمن تنظيمات التجارة الدولية للتوجه الحاصل نحو الاقتصاد الرقمى والاقتصاد المؤسسى على المعرفة ونحو راس المال الفكرى.
٤- تشريعات الأصول الاجرائية الجزائية، وتشريعات الاثبات المتفقة مع عصر الكمبيوتر والمعلومات والتى هى فى الحقيقة تطوير لقواعد الاجراءات والاثبات، لكنها ايضا تتصل عضويا بالحقوق الجديدة المعترف بها فى ميدان تقنية المعلومات.
٥- تشريعات المحتوى الضار (الحماية من محتوى المعلوماتية على الإنترنت)، ثمة اتجاهات متباينة بين توجه لدمجها مع تشريعات امن المعلومات كما فى أوروبا ، أو استقلالها عنها كما فى امريكا.
٦- تشريعات معايير الامن المعلوماتى وتطورها إلى تشريعات المواصفات القياسية لتبادل البيانات والتشفير، وثمة أيضا اتجاهات لاعتبارها جزءا من تشريعات التجارة الالكترونية فى حين هناك اتجاهات لتناول كل موضوع من

مواضيعها فى تشريع مستقل.

٧- التشريعات المالية والمصرفية فيما يتصل بالمال الالكترونى وتقنيات الخدمات المصرفية والمالية وفى مقدمتها البطاقات المالية ونظم التحويل الالكترونى والتى تطورت لتشمل اطرا جديدة فى مجال التوجه نحو الاتمته الكاملة للعمل المصرفى والمالى (البنوك الالكترونية).

٨- تشريعات الاستثمار والتجارة والضرائب والجمارك والاتصالات والانظمة الحكومية المرتبطة بالمشروعات التقنية او المتأثرة بتقنية المعلومات.

٩- تشريعات التجارة الالكترونية (التواقيع الالكترونية، والتعاقد الالكترونى، والتسوق الالكترونى)، وسنجد أن هذه الطائفة تتضمن قواعد تتصل بكافة مجال تقنية المعلومات لأنها اثارت تحديات فيها جميعا، لهذا ثمة حقيقة أن التجارة الالكترونية وحدها برغم أنها آخر حلقات تقنية المعلومات فى الوقت الراهن الا أنها الاطار الاوسع المؤهل لتوحيد قواعد قانون الكمبيوتر.

١٠- تشريعات (اتفاقيات ومعاهدات) الاختصاص والقانون المطبق على المنازعات القضائية فى بيئة الإنترنت (بشكل خاص منازعات الملكية الفكرية ومنازعات التجارة والاعمال والبنوك الالكترونية).

أمام الموجات التشريعية المتقدم الاشارة اليها، وامام هذا التطور التاريخى والحصر المتقدم لمجالات الموضوعات المتصلة بتقنية المعلومات وعلاقتها بالقانون، يرد التساؤل : ما هو قانون الكمبيوتر Computer law ، أو قانون السيبر Cyber Law؟ وماذا عن الاصطلاحات الدالة عليه؟؟ ثم ، هل ثمة اساس لبناء نظرية عامة لقانون الكمبيوتر ، ام انه سيظل مجرد مبرر لتعديل قواعد قانونية قائمة فى اكثر من فرع قانونى واكثر من تشريع فى نطاق النظام القانونى الواحد.

القواعد العامة لقانون الكمبيوتر:

ابتداء تجدر الاشارة إلى أن كلمة (سايبر لو – Cyber law) اصطلاح دال على قانون الكمبيوتر أو قانون تقنية المعلومات درج ضمن مجموعة اصطلاحات نحتت جميعها من تعبير (سيبر سبيس Cyberspace) وهذا التعبير الاخير يترجم بمعان كثيرة، ابرزها الفضاء التخيلى، أو الفضاء الالكترونى، وهو مصطلح نحته المؤلف وليام جبسون William Gibson ليشير به إلى الحقيقة التخيلية لشبكات الكمبيوتر. ويشيع استخدام هذا المصطلح كمرادف لكلمة

"الإنترنت" أو البيئة الرقمية، بل انه يحل فى الاستخدام الشائع مكان كافة التعبيرات المتصلة بتقنية المعلومات.

وقد تفرع عنه عدد كبير من الاصطلاحات فنجد تعبير (السيبر كاش – سايبركاش Cyber cash) ليدل على نظام دفع النقود بواسطة الشيكات الالكترنية أو بطاقات الائتمان وتعبير سيبر تايم Cyber time للدلالة على وقت الإنترنت من الوجهة التقنية وعلى عصر الإنترنت من الوجهة التوصيفية، وتعبير (سايبر كرايم – Cyber crime) للدلالة على الجرائم الالكترونية أو جرائم الكمبيوتر،وغيرها العشرات من التعبيرات التى تنطلق من فكرة البيئة التخيلية أو الافتراضية أو الرقمية لحقائق ومفاهيم واقعية، لهذا من المهم معرفة أن هذا الاستخدام استخدام عملى شائع، ولهذا فانه وان لم يكن بدقة الاصطلاحات الاكاديمية البديلة للتعبير عن ذات المعانى، فان استخدامها ليس فيه خطأ سيما وانه يساهم فى تقريب الموضوع إلى اذهان المتلقين الذين تشيع بينهم اصطلاحات الإنترنت ، وتخلق فى اوساطهم ثقافة خاصة بهم[٩].

وبالعودة إلى قانون الكمبيوتر ، فثمة خلط واسع فى تحديد المقصود بقانون الكمبيوتر وذلك تبعا للرؤية التى يعتمد عليها فى تحديد اقسام هذا الموضوع والاطار العلمى محل المعالجة [١٠]، وثمة ايضا تباين بشأن مشتملاته،

---

[٩]- وجدير بالذكر هنا ان كل موضوع من مواضيع العلم والفن ، جرى إختراقه بعدد من الاصطلاحات التى ترافقت مع شيوع تقنية المعلومات، ورغم وجود مدافعين عن اصول اللغة ورفضهم هذه الاختراقات التى عادة ما تكون نحتا لعدة كلمات للدلالة على استخدام معين أو مفهوم معين، فان حمى انتشار الاصطلاحات ادى إلى ان تهتم كثير من مواقع الانترنت بايراد الاصطلاحات الخاصة بالموضوع الذى تعرضه. فى هذا الحقل وفيما يتصل باثر تقنية المعلومات على الثقافة واللغة عموما واثرها من منظور عربى، ا نظر المؤلف القيم للدكتور نبيل على- الثقافة العربية وعصر المعلومات، منشورات دار المعرفة، العدد ٢٦٥ يناير ٢٠٠١.

[١٠]- انظر التباين الحاصل فى مفهوم ونطاق قانون الكمبيوتر ضمن مجموعة المؤلفات التالية :

- Barry B. Sookman, Sookman computer Law: Acquiring protecting Information Technology, Carwell Legal Pubns, April 2000.

- David Bainbridge- Introduction to computer Law, 5th edition, Finical Times Management, 2000.

فنجده عند الغالبية يتصل بجرائم الكمبيوتر وامن المعلومات ونظمها فقط انطلاقا من أن هذا الفرع القانونى انما نشأ فى معرض الحماية القانونية للمعلومات وتحديدا الحماية الجنائية. ونجده عند آخرين الفرع المتعلق بالإبداع وحماية الملكية الفكرية، لربطهم الوجود القانونى للمعلومات بنظم المعالجة ودورها فى انتاج المعرفة ولان المعلومات من حيث طبيعتها (معنوية) ، ونجده عند آخرين موضوعات مستقلة عن بعضها البعض لا يربطها الا تعلق اى منها بالكمبيوتر أو برمجياته أو الإنترنت، حتى وصل هذا التشتت إلى درجة أن تتناول بعض مواقع الإنترنت قانون الكمبيوتر حتى لو كان عقود بيع الكمبيوتر كمنقولات مادية. وبرأينا أن هذا التشتت طبيعى فى ظل عدم الانطلاق من نظرية عامة تؤطر هذا الفرع المستجد.

ولو عدنا إلى تاريخ نشأة القوانين، كل فرع على حده، لوجدناها قد نشأت ضمن تطور طبيعى تاريخى انطلق من حاجات التنظيم القانونى للعلاقات المستجدة، لتكون فى بدايتها تنظيمات جزئية ومن ثم تتطور إلى نظريات قانونية عامة فتعود القواعد الفرعية جزء من كل محكوم بالنظريات الشمولية والاكثر من هذه الفروع القانونية نشأ فى بيئة العرف القانونى وقواعد السلوك التى احتاجت فيما بعد للتقنين القانونى ووضع المدونات التشريعية أو احتاجت على الاقل إلى استقرار قضائى بشأنها، لكن تقنية المعلومات المتسارعة فى حركتها الداخلية وفيما تفرزه من تحديات وتفرضه من تغيرات فى انماط السلوك والعلاقات القانونية ، جعل الحاجة إلى التدخل التشريعى اقرب إلى الاستراتيجية المتلائمة معها من انتظار سيادة أعراف سلوكية تتحول إلى أعراف قانونية، لهذا كان نشوه هذا الفرع واقعيا اسرع من غيره.

فالقانون الجوى على سيبل المثال، لم ينشا بمجرد اختراع الطائرة، لكنه

- Emmanuel Michau, Computer Law in France, the computer law association, May 1998

- Ricardo Barretto & Ferreira da Silva, Computer Law in Latin America, The computer law Association, December, 1997.

- Vanessa Marsland, European Computer Law: An Introductory Guide, The computer law Association, December, 1996.

نشأ عند توفر الحاجات العملية إلى تنظيم استخدام الطائر وتنظيم المسئوليات القانونية المتصلة بهذا الاستخدام، وصحيح ان قواعده فى حقل المسئولية مثلا قد تكون فى غالبيتها تطبيق للقواعد القانونية العامة فى هذا المجال ، لكن كثيرا منها ايضا مثل خروجا عن القواعد العامة.

لهذا كان لزاما ان ينطلق بناء نظريات هذا القانون من خصوصية المحل الذى ينظمه، فالطائرة وهى فى حقيقها منقول مادى، لم تكن لتحتمل قواعد المنقولات فى كل الاحوال، لان ما يتصل باستخدامها مختلف عن العلاقات التى تتصل باستخدام الأموال المنقولة الاخرى.

وبفعل جهد دولى واقليمى ووطنى وتظافر الآراء القانونية والفنية وآراء قطاعات الاقتصاد الخدمى فى حقل الطيران، تبلور هذا الفرع وجمع فى اطاره قواعد عديدة انتمت إلى اكثر من فرع عام، فنجده يضم قواعد ادارية تنظيمية وقواعد تتصل بالمسئوليات والحقوق المدنية واخرى تتعلق بالحماية الجزائية، ولوعدنا إلى فحصها قاعدة قاعدة نجدها فى الغالب تمحورت حول الطبيعة الخاصة للطائرة قيمة ومهاما واستخداما وما اتصل بها من خدمات فرعية وما تعلق بها جميعا من علاقات قانونية وواجبات قانونية .

فالطائرة اساس فكرة القانون الجوى وفى نطاقها صيغت نظريات الاخطار الجوية والمسئوليات القانونية للناقل فى حقل نقل الركاب والبضائع وغيرها، ومن الطبيعى ان تصاغ العديد من قواعده سندا لنظريات قائمة فى فرع يتحقق فيه اتصال بالقانون الجوى وهو القانون البحرى، لهذا لن نجد كثيرا من التباين فى حقل التزامات الناقل الجوى والبجرى بشأن البضائع الا فى حدود تباين مميزات النقل ذاته، لكن كل هذا لا ينفى ان نظريات عامة قد صيغت لبناء هذا الفرع القانونى، والطائرة رأس الحربة فى صياغتها وليست بذاتها بقدر ما هى واسطة النقل الجوى، فما هو رأس الحربة فى صياغة قانون الكمبيوتر؟؟؟ .

ربما يكون التصور الأولى انه الكمبيوتر ؟؟ لكنه قطعا ليس التصور الصحيح إذا ما تعامنا معه كجهاز، لأن التلفاز مثلاً لم ينتج فرعاً قانونياً مستقلاً، حتى بالنسبة للإعلام وقوانينه فانه لا يمثل اكثر من واسطة من وسائط الاعلام ذاته الذى يقوم أساسه نقل المعلومات للآخرين باشكالها المختلفة مرتبطاً بالثقافة

وبحرية الرأى والتعبير. لكننا لو عدنا لمفهوم الكمبيوتر الشامل كأداة لمعالجة البيانات، لوجدنا أن (وجوده الحيوى) يتعلق بالمعلومات بأشكالها العديدة وانماط السلوك التى اتصلت بالتعامل مع المعلومات واستثمارها.

فالكمبيوتر دون قيمة إن لم تتوفر المعطيات والبرامج، والبرامج عبارة عن أوامر تنظم لتنتج برنامجا ذا هدف أما تشغيل الكمبيوتر أو إنفاذ مهمات تطبيقية فيه، إذن البرنامج معلومات. وقواعد البيانات المخزنة داخل نظم المعلومات قد تضم بيانات خام تعكس حقائق لا تتغير، كالبيانات الشخصية مثل الاسم وتاريخ الميلاد وغيرها، وقد تضم قواعد معرفية وحقائق ثابتة، كقواعد البيانات التى تتضمن حقائق علمية أو قرارات محاكم القضاء مثلاً، وقد تكون قواعد إنتاجية لمعلومات معتمدة على بيانات خام مدخله داخل النظم، ومثالها قواعد البيانات المستخدمة فى تنفيذ طلبات أو الاجابة عن تساؤلات معينة. ومواقع الإنترنت تحتوى ضررا واصواتاً وكتابات نصية، وهى جميعاً معلومات، بعضها منتج كجهد إبداعى وبعضها الاخر حقائق إعلامية أو معرفية لا أكثر.

اذن ، مادة الكمبيوتر، بل هدف وجوده، يتمثل بالمعلومات (بمعناها الشامل للبيانات والمعلومات والمعطيات) لهذا صح القول أن محل نظريات قانون الكمبيوتر هى المعلومات وهى اساس بناء قواعده، وعندما نقول المعلومات فاننا نعنيها بذاتها وبنظم معالجتها وبانماط استغلالها ، وطبائع السلوك والتصرفات المتصلة بها.

ومن الحق التساؤل ؟ لماذا اذن لا يكون القانون هذا قانون المعلومات؟ (١١).

[١١]- ورد الاشارة إلى تعبير قانون المعلومات فى العديد من المؤلفات ، وهى اما موقف للمؤلف ذاته أو مجادلة فيما يستخدمه الباحثون من اصطلاحات مع بحث حول نطاق حماية المعلومات واتجاهاته، انظر بالإضافة للمؤلفات المشار اليها فى الهامش السابق مباشرة.

- Lawrence M Hertz, The computer and the law , Mathew Bender & Company, 1999 USA.

- Peter B. Maggs, Computer Law: Cases, comments, and Questions. wads West worth, 1996.

- Computer Law Forms Hand book, Clark Boardman Callaghan, 1995.

الحقيقة أن هذا الاستخدام وفى اطار استنجاتنا المتقدمة اكثر دقة فى الدلالة على هذا الفرع، كما أن استخدام الاصطلاحين على نحو مترادف امر صحيح، لكن شيوع تعبير أو اصطلاح قانون الكمبيوتر انما نشأ عن الاهمية الاستثنائية للكمبيوتر كوسيلة لحفظ وخزن ومعالجة ونقل المعلومات، إضافه إلى أن الاعتراف للمعلومات بالحق القانونى فى الحماية والمحل القانونى للمصالح الناشئة ارتبط لدى القانونيين بوعاء المعلومة لا بذاتها فحماية حق المؤلف لم يمتد لحماية الافكار والخوارزميات انما للشكل النهائى الذى افرغ فيه الإبداع، فكانت حماية البرامج بوصفها اوامر مرتبة يتمثل الإبداع فيها فى عملية الترتيب لا فى الخوارزميات محلها، وحماية قواعد البيانات، لا يمتد للبيانات محل القاعدة بل لتصنيفها وتبويبها الإبداعى وهكذا.

ولأن اساس قانون الكمبيوتر ومبرر وجودة الحماية القانونية للمعلومات، فان قصره على جرائم الكمبيوتر المتصلة بحماية استخدام الكمبيوتر ومخزونه المعلوماتى والحق فى ملكية المعلومة ذات القيمة الاقتصادية اما بذاتها أو بما تمثلة، قد اغفل اوجه حماية اخرى وأنماطاً معلوماتية اخرى، فاغفل بذلك البيانات الشخصية مثلا، واغفل حماية انماط التعامل الالكترونى مع المعلومات،

- John Zeleznikow. Dan Hunter, Building Intelligent Legal Information systems, little Brown & company, 1994.
- Reba A. Best, D. Cheryn Picquet, Computer law and software protection., Mcfarland & company, 1993.
- G.P.V Vandenberghe, Advanced Topics, of law and Information technology, kluwer Law International. July 1989.
- A.W.Koers, Knowledge Based Systems in Law, Kluwer law International. July 1989.
- Richard L. Bernacchi, Aguide to the Legal and Management Aspects of Computer Thechnology, little Brown & Company, 1986, (2nd edition 1993).
- Colin Tapper, Computer Law, Longman 1982 (first edition 1978).
- Daniel Brooks, Computer Law, Parctising Law Inst. 1982.

واغفل العلاقات العقدية فى بيئة المعلومات، وقصره ايضا على حماية الملكية الفكرية، يحقق الحماية فقط لأوعيه المعلومات واشكالها النهائية المنطوية على عنصر ابداعى، ويغفل حماية استخدام نظمها ويغفل حماية المعلومات ذات القيمة الاقتصادية.

ومثل هذا القول ينسحب على اى رأى يحصر قانون الكمبيوتر بأحد مجالاته ليكون عاجزا عن شمول مفردات حماية المعلومات.

وبالتالى المعلومات اساس الحماية ولن نجد جدلاً أكثر من الجدل فى تحديد مفهوم المعلومات وتعريفها وما يتصل بها من حقوق[١٢] على مدى اصبح من الشائع ان نسمع عبارة (المعلومات عصية على التعريف) وتبعا لهذا الموقف ايضا سمعنا ونسمع ان (جرائم الكمبيوتر تأبى التعريف) (والمعلوماتية تأبى الخضوع لفكرة التعريف) وهكذا.

والحقيقة أن كل هذا الجدل مصدره التباين فى العلم موضع البحث عند الاتجاه للتعريف، فعلم المعلومات ربطها دوما بمادة المعرفة، وعلم الاعلام ربط المعلومة بوسائل توصيل المعلومة وبالاتصال ومهاراته، وعلم الحوسبة ربط المعلومة بانشطة المعالجة وسلوكيات استثمارها ، وعلم القانون تعامل مع المعلومة فى نطاق المصلحة محل الحماية والحق الذى يحميه القانون، وثمة تركيز على تحديد ما يتعلق أو يتصل بها من مصالح أو حقوق وما يرد عليها من قيود، وتقييم الموقف من الاعتراف بهذه المصالح أو الاقرار بهذه الحقوق.

[١٢]- فى الوقوف على اتجاهات تعريف المعلومات وما يتصل بها من حقوق انظر، د/ احمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلى، دار النهضة العربية، ٢٠٠٠، ص ٢٥ وما بعدها، وكذلك د. سعيد عبد اللطيف حسن، اثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت ، ط١ دار النهضة العربية، ١٩٩٩، القاهرة، ص ٣١ وما بعدها، د/ محمد شامى الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات ، ط٢ دار النهضة العربية، ١٩٩٨، وكذلك هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات مكتبة الآلات الحديثة، ١٩٩٢.

إذا انطلقنا من التحديد المتقدم والحقائق التاريخية لنشوء هذا الفرع، فاننا نصل إلى أن قانون الكمبيوتر هو ذلك الفرع الذى ظهر بسبب المسائل القانونية المستجدة والفريدة التى نشأت من استخدام الكمبيوتر والإنترنت، ويتميز عن غيره من الفروع بانه متعدد الاثر والتاثير، فهو يطال فروعا قانونية عديدة من الفروع المعروفة ضمن تقسيمات القانون، ويشمل فى نطاقه مسائل التعاقد، والاثبات، والضرر، والملكية الفكرية، والتوظيف، والدستورية، والبنوك والجزائى، والاجراءات والمدنية.. الخ.

ومن جهة اخرى وبرغم اتساع وتشعب مسائلة، فانه فرع ضيق يتعلق بمساحة ضيقة هى المسائل المرتبطة بالكمبيوتر (Computer- related topics)، على أن يكون مفهوما أن الكمبيوتر ليس مجرد الحوسبة ومعالجة البيانات، بل المفهوم الشامل للكمبيوتر كنظام ادخال وخزن ومعالجة وتبادل ونقل للبيانات ، اى يشمل وسائل الحوسبة والاتصالات بتفرعاتها العديدة، والمعبر عن دمجهما فى هذه المرحلة بشبكات المعلومات وفى مقدمتها الإنترنت.

والاطار الضيق لقانون الكمبيوتر– من حيث يتعلق بالكمبيوتر واثره تمتد بالمقابل إلى مساحة رحبة من الاجابة عن تساؤلات عديدة، تغطى مسائل متنوعة، تتعلق بمسئوليات مختلفة المنشا والمصدر: كيف احمى برنامج الكمبيوتر؟ هل يمكننى مقاضاه مزود خدمة الإنترنت على انقطاع الخدمة؟ هل يمكننى مراقبة اداء الموظفين عبر البريد الالكترونى ورسائلهم فى بيئة العمل؟ هل ابرام العقد على الإنترنت صحيح؟؟ كيف السبيل لانشاء موقع على الإنترنت وحماية محتواه من القرصنة؟ هل ارسال رسالة ممازحة عبر البريد الالكترونى وتكرار ذلك بشكل يثقل نظام المتلقى ويزحمة يشكل مسئولية قانونية ؟ كيف يجازى من يطلع على اسرار مؤسسته التجارية عبر الدخول إلى نظام الكمبيوتر؟؟ هل تعتبر الرسائل الموقعة رقمياً رسائل صحيحة موقعة منى؟؟ هل انزال مقطوعة موسيقية عن الشبكة ووضعها على كمبيوتره الشخصى يخلق مسئولية قانونية؟

إن الكمبيوتر اكثر من مجرد تقنية جديدة، انه وسيلة مؤثرة فى تغيير اتجاهات الثقافة والسلوك انه يمس كل ما نفعل ويخلق عدد من المسائل القانونية

خلال ذلك، حتى أن المفاهيم القانونية الرئيسية والبديهية قد تاثرت، فحتى وقت قريب ما كان احد يتصور أن الالة ممثلة بالكمبيوتر ، قد تقوم بتصرفات أو تبرم عقودا، لكن الان ثمة العديد من نظم الكمبيوتر الذكية المرتبطة بشبكة الإنترنت تقوم بابرام تصرفات وعقود دون تدخل بشرى، الطلبات تجرى من كمبيوتر لكمبيوتر، البضائع تنقل والنقود تتداول.. ماذا يحصل عندما يحدث خطا فى الكمبيوتر أو فى انفاذ اى كمبيوتر للصفقة على نحو خاطئ؟ هل يخل الكمبيوتر بالعقد ؟

أن مبالغ ضخمة تستثمر فى حقل التكنولوجيا ، انشاء وشراء الشبكات واطلاق مواقع الإنترنت (web sites)، الاستثمار فى قواعد البيانات وعمليات المعالجة، البرمجة وتطوير البرمجيات، الخدمات التقنية بمختلف انواعها، ولو دققنا فى هذا الانشطة لنتبين – مثلا- الجهة التى تقوم بتنظيم عقودها ، لاكتشفنا حقيقة غريبة، وهى أن غالبية العقود- خاصة التى تعقد فى البيئة العربية- يضعها اداريون وتقنيون وماليون ولكنهم قطعا ليسوا من مجتمع القانون المختص بهذه الاعمال .. لماذا؟ لأن هذه عقود تتطلب لإعدادها فهماً وادراكا للجوانب التقنية، ادراكا للجوانب العملية لتصرفات المستهلكين وجهات الانتاج والخدمة، والاطلاع على الجديد من القوانين، وليس فى البيئة العربية فحسب، بل حتى فى دول متقدمة، ثمة عقود ضعيفة البناء، فقيرة المحتوى ، مع أن جملة هذه الموضوعات تفرض عقود اكثر عمقا وتعميقا لانها ستمثل فى الحقيقة القانون الذى يحكم النزاع وضعف العقود وثغراتها هو الذى يخلق منازعات متعددة فى الواقع العملى.

والأصل أن المحامين اذ يتولون اعداد العقود فانهم يهدفون إلى منع النزاع- على الاقل فى المسائل الرئيسية- وترك جانب قليل ليكون محل خصام ، ولا يعقل أن تكون التكنولوجيا عاجزة عن منع النزاع أو بشكل اسوء، أن تكون هذه العقود السبب فى حصوله عند عدم دقتها وعند اتصافها بالعمومية بما تفتحه من فرصه لكل طرف للتشبث بما يخدم مصلحته ويبرر مسلكة

إن عقود الكمبيوتر (computer contracts) والخدمات التقنية الجيدة- كعقود توريد الاجهزة، ونقل المعرفة، وعقود البرمجيات ورخصها،

وعقود الخدمات التقنية فى المؤسسات المالية أو عقود خدمات بناء المواقع وادارتها ، والدعم والتطوير وعقود خدمات الاعلان الالكترونى .. إلخ - هى التى تجيب عن الاسئلة الرئيسة فى المجال أو الموضوع الذى تعالجه: - ما الذى يؤديه النظام التقنى؟ ما هى سرعة الاداء؟ كيف تؤدى الخدمة؟ ما هى خيارات المستخدم؟ ما هو الفحص أو المعاينة المقبولة لقبول الاجهزة أو البرمجيات الجديدة؟ ما هى كفالة الضمان وما هى شروطها ومدتها ونطاقها؟ ما هى حدود المسئولية، اهى مطلقة ام مسئولية محددة، ووفقا لماذا هى محددة، وما مقدارها، والى اى مدى يتفق تحديد المسئولية مع قواعد النظام القانونى؟ هل ثمة قيود على تحديد المسئولية فى بيئة الكمبيوتر؟ ماذا عن قواعد حماية المستهلك؟ من يملك حقوق الملكية الفكرية؟ لمن تؤول عند انتهاء الشركات خاصة شركات الاعمال غير المسجلة؟ ما هى معايير الخدمة التقنية، السرعة، مدة الانقطاع، المسئولية عن الانقطاع؟ اين يتم حل النزاع، كيف يتم حله، اى قانون يطبق.

وقانون الكمبيوتر يختص ايضا بشئون الشركات العاملة فى حقل صناعة الكمبيوتر والبرمجيات والاتصالات أو النقل، شركات تقنية المعلومات (It companies) ، كمزودى خدمات الإنترنت ("ISP" Internet service provider) ومنتجى الكمبيوتر والبرمجيات (Manufacturers) والموزعين (Distributors) ومطورى البرامج ومواقع الإنترنت (Software and web site developers) ومحللى النظم والشبكات واختصاصيى تكاملها (Network integrators) وغيرها فى حقل صناعة الكمبيوتر والشبكات والبرمجيات وجميعها تتطلع إلى قانون الكمبيوتر لتحمى نفسها وتحقق اغراضها من خلال المشورة القانونية التى يقدمها قانون الكمبيوتر. انهم يحتاجون القانون من اجل عقد الصفقات، رخص الملكية الفكرية، حقوق التوزيع والاعلان، قانونية ما يقدمونه من مواد أو خدمات أو يحتاجونه لينظم لهم عملية اطلاق خدمات تجارية الكترونية مثلا أو خدمات الكترونية اخرى. قد تحتاج شركات تزويد خدمات الإنترنت لتعرف مسئوليتها تجاه المشتركين معها، كالمسئولية عن عدم وصول البريد الالكترونى، أو مسئوليتهم عند قيام احد مشتركيهم بارسال رسالة تهديد أو رسالة مساس بسمعة الغير أو قيامه باى عمل غير قانونى عبر الشبكة من خلالهم ، وقد تحتاج هذه الشركة معرفة موقف القانون عندما تطلب منها جهة تحقيق ، كالشرطة الفدرالية الامريكية مثلا (FBI) المعلومات السرية عن المشتركين ومراسلاتهم. وقد

يحتاجون القانون عند ابرام صفقات البيع والشراء والاندماج والمشاركة المتصلة باعمالهم.

والاختصاص بنظر منازعات الإنترنت والقانون الواجب التطبيق ومشروعية امتداد التحقيق والتفتيش والضبط إلى خارج الحدود والاعتراف القانونى بوسائل التعاقد الالكترونية والمراسلات الالكترونية وحماية البيانات الشخصية من انشطة الاعتداء، سواء من الغير ام من جهات معالجة هذه البيانات والانماط الجديدة فى الاستيلاء على المال عبر استخدام الكمبيوتر وانشطة المساس بنظم الكمبيوتر والمعطيات المخزنة فيها وموقف المحاكم من منازعات الإنترنت، قبولا واختصاصا ومحتوى.. أنها جميعا من مسائل قانون الكمبيوتر اذن .

فقانون الكمبيوتر هو كل شئ عن تآلف الكمبيوتر والإنترنت والفضاء الافتراضى مع النظامين الاقتصادى والقانونى للدولة، انه مصدر خلق احكام واقرار نتائج قابلة للادراك والتنبؤ بها فى ظل التصرفات الافتراضية وفى اطار البيئة الافتراضية، وذلك من خلال قواعد عقدية وقانونية واضحة. ويعد قانون الكمبيوتر لذلك، الفرع القانونى الذى يعنى بالقواعد القانونية الناجمة عن استخدام الكمبيوتر بمفهومه الواسع (الدمج بين الحوسبة والاتصالات ومحتوى المواقع المعلوماتية) وتتصل بعمليات الكمبيوتر أو شبكات المعلومات (وتحديدا الإنترنت) وبأى تصرف أو سلوك فى هذا الاطار يتصل بالمعلومات ونظمها[١٣].

[١٣]- انظر: Mark Grossaman على الانترنت حيث يهتم بقانون الكمبيوتر منذ عام ١٩٩٦- www.mgrossmanlaw.com وانظر ايضا موقع :

The cyberlaw encyclopedia. http://gahtan.com\techlaw

الفصل الثانى
مدلول الجريمة المعلوماتية

تمهيد:

يؤكد الخبراء أن الجرائم الالكترونية تزداد كلما توغل العالم فى ازدياد استخدام الإنترنت، فالإنترنت بوابة بلا حراس بل هى ساحة إجرام تتحدى الاجهزة الامنية بما لديها من ثغرات قانونية ضخمة، مما أتاح لمافيا الجرائم الالكترونية التجول خلالها دون رقيب أو حسيب، وتكشف الخصوصية والسرية التى تنطوى عليها لغة الكمبيوتر، وكذلك يمكنها نقل المعلومات المحظورة بمجرد الضغط على زر بلوحة المفاتيح، دون أى مجهود ودون اى خوف من العقاب.

مدلول الجريمة المعلوماتية:

الجريمة المعلوماتية لها مسميات كثيرة، فهى جريمة الكمبيوتر والإنترنت، والبعض الأخر يطلق عليها الجريمة الالكترونية، وهى جريمة إساءة استخدام تقنية المعلومات، وقد بذلت محاولات متعددة تسعى إلى ايجاد تعريف مناسب لهذه الجريمة وان كانت جميعها لا تخرج عن أحد اتجاهين:

<u>الإتجاه الأول</u>:

يرى انصار هذا الاتجاه أن الجريمة المعلوماتية هى " كل سلوك غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية، وملاحقته وتحقيقه من ناحية اخرى"

وبمعنى آخر هى" نشاط إجرامى تستخدم فيه تقنية الحاسب الآلى بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الاجرامى المقصود"[١٤].

وطبقاً لهذا التعريف فانه يجب أن تتوافر معرفة التكنولوجيا الخاصة بالحاسبات الآلية بدرجة كبيرة، ليس فقط من أجل ارتكابها ولكن أيضا من أجل التمكن من ملاحقتها والتحقيق فيها على نحو صحيح، أى أن يكون مرتكب الجريمة المعلوماتية والقائمون على ملاحقتها على درجة كبيرة من العلم بهذه التكنولوجيا.

ويرى مؤيدو هذا الإتجاه، أن الجرائم التى تفتقر إلى هذه الدرجة من

---

[١٤]- انظر: د/ محمد الامين البشرى- التحقيق فى جرائم الحاسب الآلى – بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت-كلية الشريعة والقانون-جامعة الإمارات مايو ٢٠٠٥ صفحة ٦.

المعرفة تعد جرائم عادية تتكفل بها النصوص الجنائية العادية، ولا داع اطلاقا لنصوص جديدة اخرى ،وذلك خلافا للجرائم التى تتوافر لها هذه المعرفة حيث تحتاج نصوصاً جديدة تتلاءم مع طبيعتها.

ويذهب البعض من مؤيدى هذا الاتجاه، إلى أن الجريمة المعلوماتية هى" كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومة المخزنة داخل الحاسب الآلى أو تلك التى يتم تحويلها عن طريقة".

ومع تقديرنا لهذا الرأى ، وبقدر وجاهته الا اننا نرى عدم تطلب القدر الكبير من المعرفة التقنية لارتكاب الجريمة المعلوماتية، فجريمة اتلاف البيانات المخزونة وسرقة المعلومات، لا تتطلب قدراً كبيراً من العلم بهذه التكنولوجيا، وكذلك هذا الاتجاه يخرج من نطاق الجريمة المعلوماتية كثير من الافعال غير المشروعة جنائياً، والتى تستخدم الحاسب الآلى كأداة لارتكابها كالاحتيال المعلوماتى واشاعه الفواحش والافعال المخلة بالآداب العامة عن طريق الحاسب الآلى[١٥].

الإتجاه الثانى:

ذهب بعض أنصار هذا الاتجاه إلى القول بأن الجريمة المعلوماتية هى كل فعل غير مشروع يتم بمساعدة الحاسب الآلى، أو هى كل جريمة تتم فى محيط الحاسبات الآلية.

وهذا الاتجاه يوسع كثيرا من مفهوم الجريمة المعلوماتية.

ويرى البعض الاخر من أنصار هذا الاتجاه أن الجريمة المعلوماتية هى " كل تلاعب بالحاسب الآلى ونظامه من اجل الحصول بطريقة غير مشروعه على مكسب للجانى أو الحاق خسارة بالمجنى عليه".

وانطلاقا مما تقدم يمكن تعريف الجريمة المعلوماتية بانها" كل نشاط اجرامى يؤدى فيه نظام الحاسب الآلى دوراً لإتمامه على أن يكون هذا الدور على قدر من الأهمية[١٦].

---

[١٥]- أنظر د/ نائلة عادل محمد فريد – جرائم الحاسب الإقتصادية (دراسة نظرية وتطبيقية) دار النهضة العربية- القاهرة ، ٢٠٠٤، صفحة ٢١- ٢٣.

[١٦]- أنظر د/ نائلة عادل محمد فريد – المرجع السابق ، صفحة ٢٥- ٢٦ .

ولا يختلف الامر سواء كان الحاسب الآلى اداة لإتمام النشاط الاجرامى ام كان محلا له، ففى جريمة الاتلاف قد ينصب نشاط الفاعل على الحاسب الآلى ذاته أو على اى من مكوناته المادية وفى هذه الالة لا يعدو الحاسب الآلى أن يكون محلاً مادياً ينصب عليه سلوك الجانى الإجرامى دون أن يكون لوجوده اى دور فى الجريمة المعلوماتية، أما إذا انصبت فعل الإتلاف على المكونات المنطقية للحاسب الآلى (كالمعلومات أو البرامج أو انظمة التشغيل) فان للحاسب ونظامة فى هذه الحالة دوراً مهماً لإتمام الجريمة المعلوماتية

مدلول الجريمة الالكترونية:

تعتبر الجريمة الالكترونية من أخطر الجرائم التى ترتكب عن طريق الإنترنت نظراً لتوسع استخدامها وتشعبها فى شتى المجالات، وكذا إتساع نطاق مستخدمى شبكة الإنترنت بعد أن كانت قاصرة على البحث العلمى، واصبحت الشبكة مجالاً خصباً لنقل المعلومات الخطرة والهامة والحيوية سواء على المجالات المخابراتية أو الامنية أو الاقتصادية، والجريمة الالكترونية تعد نوع من انواع جرائم المعلوماتية.

والجريمة الالكترونية يمكن وصفها بانها: كل فعل يستهدف القضاء على استخدام التكنولوجيا الحديثة عبر الوسائط الالكترونية " ومع غزو الإنترنت دول العالم أصبح من الصعوبة بمكان ضبط وكشف هذه الجرائم نظراً لكونها عابرة للحدود ولا دين ولا وطن لها وتتم بسرعة فائقة دون رقيب أو حسيب ودون رقابة من اى دولة مما ادى إلى ارتكاب كافة صور النشاط الاجرامى المتعارف عليها عبر الإنترنت حتى القتل والسطو على برامج الحاسب بغرض سرقة البيانات وقاعدة المعطيات المعلوماتية حتى السرية منها واستخدامها فى التجسس أو تلك المتعلقة بالقرصنة والسطو عل الاموال إلى جانب ظهور الارهاب الالكترونى وتهديد الامن القومى للدول ، وكذا جرائم الآداب العامة والمساس بالاخلاق من خلال الاباحية الالكترونية التى تجسدها المواقع الجنسية الاباحية[١٧] ، خاصة الموجهة منها للاطفال والمقدرة باكثر من الف موقع يقدم مواد جنسية إباحية خاصة بالاطفال دون سن البلوغ يتم فيها استخدام دعارة الاطفال والنساء[١٨] ، سواء بالغين أو قصر عن طريق تصويرهم مباشرة أو بالمحاكاة والتمثيل الرقمى للصورة باستعمال وسائل الترغيب والترهيب بالإغراء والتحذير أو التهديد.

---

[١٧]- انظر: د/ سعيد عبد اللطيف حسن – الجرائم الواقعة فى تكنولوجيا المعلومات – كلية الشريعة والقانون – القاهرة – ١٩٩٩.

[٢]- انظر: د/ مدحت رمضان- جرائم الاعتداء على الاشخاص والانترنت – دار النهضة العربية – ٢٠٠٠.

ويمكن القول بان الجريمة الالكترونية الخالصة تنطوى على ست خطوات اساسية[١٩] يتم تنفيذها آلياً بواسطة برنامج أو عدة برامج، دون تدخل العنصر البشرى وهذه الخطوات على النحو التالى:

١-البحث عن نظام الحاسب الآلى الذى يحتوى على المعلومات أو البرامج المطلوبة.

٢- الوصول إلى نقاط الضعف فى النظام الذى يحتوى على هذه المعلومات أو البرامج.

٣- الاستفادة من هذه النقاط للدخول إلى النظام ثم التحكم فيه.

٤- تنفيذ السلوك الإجرامى الذى تم التخطيط له وتحديده مسبقاً.

٥- تحويل هذا السلوك إلى ربح غير مشروع يحصل عليه الجانى أو إلى خسارة تلحق بالمجنى عليه.

٦- إخفاء جميع الادلة تجنباً لكشف الفاعل وسلوكه الإجرامى.

وانطلاقا مما تقدم ، فإننا نتناول هذا الفصل على مبحثين على النحو التالى:

المبحث الأول: ماهية المعلومات

المبحث الثانى: خصائص الجريمة المعلوماتية.

١٩- أنظر د/ نائلة عادل محمد فريد – مرجع سابق، صفحة ٢٩، ٣٠ .

المبحث الأول
ماهية المعلومات

المعلومات، هل هى ، مال، شئ ، شئ ذو قيمة، كيان، كيان معنوى. هل لأنها تتصل غالبا بوعاء تفرغ فيه ترتبط عضويا بوعائها لذا فهى شئ مادى بالنظر للوعاء المفرغة فيه؟

أن المعلومات ذات طبيعة معنوية، تستقل تماما من حيث الاصل عن الوعاء المفرغة فيه وتعدو النظرة قاصرة إذ اتجهت نظريات قانون الكمبيوتر نحو حماية المعلومات وفق وعائها.

والمعلومات شائعة من حيث الاصل ، وحصيلة تراكم معرفى بشرى ، ومن هنا ينشأ لكل فرد الحق فى الوصول اليها ، ويتيعن ان يكفل حق انسيابها وتدفقها ، وهذا هو جوهر واساس فكرة الحق فى المعلومات.

لكن المعلومات فيما اتجهت اليه انشطة تقنية المعلومات: -

اولا: أما أنها امست بذاتها ذات قيمة اقتصادية عالية تزداد يوما بعد يوم، لذا وصفت وتوصف بأنها المال، والمال من حيث الاصل يحظى بهذه الصفة لإتصاله بحق التملك، ملكية فرد أو شخص للمال، فمتى ما كانت المعلومات مال فانها قابلة للتملك وهو ما يفرز مفهوم الحق فى ملكية المعلومات.

ثانيا: أو أنها – اى المعلومات – قد تتصل بشخص دون غيره عندما تتعلق ببياناته الاسمية أو الشخصية، لكنها تستخدم من الغير، وبالذات السلطات، لاغراض تتصل بالنشاط الاجتماعى والاقتصاى والسياسى فى الدولة، من هنا تنشئ المعلومات حقا فى السيطرة عليها، وحق فى استخدامها ضمن قيود وضوابط، وهنا تبدأ وتنتهى حدود الحق فى الخصوصية المعلوماتية، أو الحق فى حماية البيانات الشخصية.

ثالثا: والمعلومات قد تكون الخلق الإبداعى للفكرة أو الابتكار فى تنظيم الحقائق والاوامر، فنكون امام مصنفات وليده الاداء الإبداعى لعقول المؤلفين والمخترعين تمثل وعاء المعلومة، فتكون لذلك وبما انطوت عليه من عناصر تتطلبها نظام الملكية الفكرية، مادة حق الملكية الفكرية وموضعا للاستئثار المعنوى والاستغلال المادى، فتخلق بذلك الحق فى الملكية الفكرية للمصنفات المعلوماتية.

والقانون ليس بوسعه ان يكون وسيلة تنظيم إلا لحق يعترف به ويكفله القانون، وليس ثمة حماية الا حيث تتوفر المصلحة التى يحيمها القانون، لهذا كان وجود قانون الكمبيوتر مرتبطا بالاعتراف بالحق فى المعلومات، انسيابها وتدفقها وقدرة الفرد على الوصول، لكن هذا الحق يثير اشكالية نطاق السيطرة على المعلومات عبر ما سيوفره الاعتراف بهذا الحق من مكنات وسلطات قانونية ، هذه السيطرة التى تتعارض جوهريا مع مفهوم الحق فى شيوع المعلومات وقدرة اى فرد فى الحصول عليها، وهذا إلى جانب ما تتصف به المعلومات من شمولية تمتد للافكار والحقائق كان وراء دعوات عدم إخضاع الحق فيها لأية قيود. لكن الحقيقة ان ما ارتبط بهذا الحق من حقوق اخرى كالحق فى ملكية المعلومات والحق فيما يتصل بها من حقوق فكرية والحق فى الخصوصية انما هى ليست قيودا على الحق بالمعلومات بقدر ما هى تنظيم للمكنات والسلطات التى تقع فى نطاق الحق فى المعلومات وتنظيم للمصالح المعترف بها قانونا فى نطاق هذا الحق.

اذن، المعلومات كيان معنوى، يتعين الاعتراف بحمايتها بهذه الصفة وبما يتصل بها من سلوكيات واداء وانشطة استثمار، تماما كما تم الاعتراف بالمال المادى وخضع لقواعد ونظريات فى المجالين المدنى والجزائى، وأساس حماية المعلومات توفير الاطار القانونى المشابة (من حيث شموليته ونطاقة وفعاليته) لذلك الذى وفرته التشريعات للمال المادى. والحق فى المعلومات يوجب اقرار مبادئ كفالة حرية الوصول للمعلومات واقرار قواعد بشأن ضوابط استخدامها والاطار القانونى لممارسة المكنات والسلطات المتصلة بها.

وفى اطار الحماية القانونية للمعلومات، ثمة مصلحة حقيقة يتعين ان يحميها القانون وهى حق الافراد فى المعلومات ، وحقهم فى سلامة ومشروعية

التعامل مع بياناته الشخصية، وحقهم فى ثمرة ابداع عقولهم المتصلة بنطاق المعلومات والمفرغة ضمن مصنفات تحميها قواعد الملكية الفكرية، وحق مالكى المعلومات (باشكالها المختلفة) المصنفة اوالخاصة بنشاطهم الاستثمارى أو التجارى وادارتهم للمعلومات التى تمثل راس المال الفعلى لمشروعاتهم، وحق الفرد فى سلامة ما يتعامل معه من معلومات سواء المرسلة منه ام المستقبلة ام المخزنة فى نظامه التقنى، واذا ما حولنا هذه الحقوق إلى مسميات فاننا نكون امام: الحق فى المعلومات، الحق فى ملكية المعلومات، الحق فى الملكية الفكرية للمعلومات، الحق فى الخصوصية المعلوماتية، الحق فى ادارة المعلومات، الحق فى امن التعامل المرتكز على المعلومات.

هذه هى المصالح المتعين حمايتها والحقوق المتعين الاعتراف بها، فاذا ما اردنا تحويلها لقواعد (عملية) تتصل بالمعلومات للانطلاق فى رسم ملامح النظرية العامة للمعلومات فاننا نكون امام الاسس العامة التالية (المتعين اقرارها فى النظام القانونى) :

١- ان الفرد من حيث الاصل له الحق فى الحصول على المعلومات ، وتظل الحقائق والافكار العامة ملكا شائعا للبشرية لا ترد عليها مكنات قانونية تحد من الافادة منها ولا سلطات استئثارية الا متى ما اتصلت بجهد خلقى (ليس هو دائما المفهوم المقرر فى نظام الملكية الفكرية فحسب) يبرر الاقرار بمصالح وحقوق ترتبط بصاحب الجهد الخلقى المتصل بها. فالافكار حول تصميم موقع الإنترنت تظل افكار شائعة لا يستاثر بملكيتها احد لكن متى ما تحولت إلى انماط خلقها مصمم موقع ما كانت ملكا فى اطارها الإبداعى هذا للشخص الذى ابتكرها ، والخوارزميات المستخدمة فى البرمجيات لا يدعى ملكيتها احد، لكن ورودها ضمن تبويب معين ينتج برنامجا مبتكرا تخلق للشخص الذى قام بذلك مكنة الاعتراف بحقة فى نسبة هذا الإبداع له وفى حماية استغلاله المادى، وهكذا.
٢- ان البيانات الشخصية عنصر من عناصر حماية السرية الشخصية واحترام الحياة الخاصة يتعين ان تخضع من حيث نطاق الحماية لما خضعت له عناصر حماية الخصوصية المادية ، المسكن والمراسلات وغيرها.
٣- ان المعلومات ككيان معنوى لها ذات القيمة الاقتصادية للمال المادى، يتعين

ان تخضع لاحكامه وتعامل تماما كما يعامل ، فتحيطها حماية ذات الحقوق المقررة على المال المادى ويعترف لها بذات المصالح التى يعترف بها القانون للمال المادى.

٤- فى نطاق التصرفات المدنية والتجارية ، فان السلوكيات والتصرفات القائمة فى البيئة الرقمية (بيئة الكمبيوتر والإنترنت) يتعين ان تكون مقبولة ومعترف بها تعبيرا عن الارادة وعن الالتزام القانونى تماما كتلك التصرفات المعتبرة والمقبولة فى البيئة الحقيقية متى ما تحقق لها عنصر القدرة على التعبير بشكل صحيح منتج لاثره.

٥- وفى نطاق الحماية الجنائية يتعين الاقرار بصلاحية المعلومات كمحل للحماية من أنشطة الاعتداء كافة، تماما كما المال المادى المحمى ضمن نصوص وقواعد حماية الاموال، ويتعين الاعتراف لمحيط المعلومات ووعائها التقنى بالصفة المقبولة لخضوعه للتصرفات التى ترتكب فى بيئة المحرر الكتابى والمستندات الخطية. ويتعين المساواة بين السلوكات المادية فى انتهاك السرية وبين السلوكيات المعنوية فى انتهاك الخصوصية.

٦- أن محل الجريمة المعنوى له ذات القيمة المعترف بها للمحل المادى للجريمة والسلوك المعنوى للجريمة تقوم به الجريمة تماما كما تقوم بالسلوك المادى فعلا وتركا.

٧- ان قواعد الضبط والتفيش فى البيئة الرقمية يتعين ان تتناسب مع مميزات هذه البيئة تماما كما تناسبت قواعد الضبط والتفتيش فى الوسط المادى مع مميزات وسلوكيات هذا الوسط.

٨- الادلة ذات الطبيعة الالكترونية يتعين مساواتها بالادلة ذات الطبيعة المادية – الادلة القائمة على الكتابة والورق – من حيث المقبولية والحجية.

٩- كلما كان التصرف المادى فى البيئة الواقعية محل اعتبار يتعين الاعتراف بما يقابله من تصرف معنوى فى البيئة الرقمية، فالتوقيع الالكترونى يقتضى مساواته بالتوقيع المادى. والتصديق الالكترونى يتعين مساواته بالتصديق المادى، وهكذا شريطة ان تحقق البيئة الرقمية من حيث المعايير والاجراءات المتصلة بالسلوكات المعنوية أو سلوكيات البيئة الافتراضية ما يوفر الثقة التى تحلت بها السلوكيات المادية.

١٠- ان البيئة الرقمية متى ما تحقق نمط ومعيار اجرائى يكفل لها الموثوقية والثقة بالسلوك فى بيئتها والاطمئنان للدليل المستخلص من وسائلها يتعين

ان تعامل كالبيئة الحقيقية، وفى نطاقها يكون الحق محل اعتراف وتكون المصلحة موضع تقدير وتكون القاعدة القانونية منطقية اذ لم تقبل تمييزا بين بيئتين توفر لهما ذات المعيار من حيث الثقة وذات العناصر من حيث الاطمئنان.

١١- ان المعلومات بذاتها وبما يتصل بها من سلوكيات متى ما تحقق الاعتراف القانونى بكيانها والاعتراف بما يتصل بها من تصرفات وما تنشئها التصرفات هذه من اثر ونتائج ومسئوليات، وما يتعق بها من حقوق ومصالح ، حققت الاسس القانونية المقر بها ضمن قواعد كافة فروع التشريع الدستورية والمدنية والتجارية والمالية والادارية والجزائية وتشريعات حماية المستهلك، المتعلقة بالتصرفات المادية والمحل المادى والآثار الناتجة عن هذه السلوكيات والمراكز القانونية الناشئة عنها.

١٢- ان المعلومات مال، والتصرفات المعلوماتية ذات وجود واثر، فلا يتعين عندها ان تحرم من التنظيم التشريعى لانها لدى الكثيرين افتراض ووهم. وبنفس الوقت لا يتعين ان تشقى القواعد القائمة فى لى النصوص وتطويع النظريات القائمة لتستوعب المعلومات خاصة بعد ان تحقق اثرها كعماد للاقتصاد الرقمى، ويتعين ان تصاغ النظريات بمرونة تستوعب القادم الجديد فى عصر المعلومات ووسائلها فتحظى بشمولية المعالجة لتحقق سرعة الاستجابة فى مرحلة اصعب ما فيها ادراك سرعة التغير وولادة الانماط المستجدة. ولا يتعين ان يحتج بالمتغيرات للهروب من مسئوليات التنظيم التشريعى، لان الأسس للمتغيرات امست واضحة فكثير من المستجدات لا تؤثر فى صحة القواعد القائمة وغالباً ما قد يكفى معها تطوير الاطار الاجرائى وليس الموضوعى، واذا كان ثمة حاجة لمواكبة التشريع للتغيير فلن تكون أوسع أثراً أو نطاقا مما شهدته التشريعات التقليدية ذاتها من تغيرات بسبب اثار العصر ومستجداته.

ومتى ما تم الاستناد إلى مثل هذه الأسس العامة جرى فض حالة التشتت والتناقض فى معالجة قانون عصر المعلومات (قانون الكمبيوتر) وكان الجواب لكل اطار فرعى قد توفر ضمن القواعد الكلية، وللتاكد من صحة النتائج فاننا نتساءل: هل تكفى هذه الاسس لمواجهة جرائم الكمبيوتر المتطورة من حيث نمطها واسلوبها يوما بعد يوم؟؟

الاجابة طبعا بالإيجاب ، لان مانع حماية المعلومات من خلال النصوص القائمة فى قوانين العقوبات هو ان النصوص تعاملت على مدى الزمن الماضى مع المال المادى والمحرر المادى والسلوك المادى وهكذا، فان قبلت المعلومات محلا صالحا للجريمة، اما بالنص الخاص أو بالنص العام الذى يساويها بالمال المادى، واعتبرت السلوكيات المعنوية فى بيئة الإنترنت والكمبيوتر سلوكيات صالحة لارتكاب هذه الجرائم والجرائم التقليدية، واذا ما قبل الدليل الالكترونى كدليل على إثبات الجرم ، واذا ما تحققت قواعد تفتيش وضبط تراعى الطبيعة التقنية لبيئة جرائم الكمبيوتر، كانت جرائم الكمبيوتر محل تنظيم وتكون الحماية من مخاطرها قد تحققت.

المبحث الثانى
خصائص الجريمة المعلوماتية

سبق القول ان التطور الحاصل فى تكنولوجيا الاعلام والإتصال وظهور الشبكة العالمية (الإنترنت) ، بكل ما حملته من تقدم وخدمات، لم يمر على العالم بسلام، لانه بقدر ما احدث آثار إيجابية وغير نمط حياة المجتمعات وساهم فى التطور والرقى، بقدر ما كان له أثر سلبى على حياة الناس ومصالح الدول باسرها، كل هذا تجلى فى تطويع الإنترنت والوسائل الالكترونية، لتكون عالماً جديداً لتظهر إلى الوجود الجرائم الالكترونية أو الجرائم المعلوماتية، وهذه الجرائم لها طابعاً قانونياً خاصا يميزها عن غيرها من الجرائم التقليدية.

ويمكن القول بأن هناك العديد من السمات التى تتميز بها الجريمة المعلوماتية اهمها:

بداية نشر إلى أن جرائم الحاسوب من الجرائم العابرة للحدود السياسية Transnational، اذ بالامكان تصور ارتكاب هذه الجريمة فى دولة ما وتتحقق نتائجها فى دولة أخرى، فتباعد مكان موقع الجريمة عن مكان نتائجها يثير مشاكل عديدة من حيث القانون الواجب التطبيق والإجراءات الجنائية وغير ذلك من المسائل القانونية.

وتتميز هذه الجريمة أيضا بسرعة تنفيذها حيث يمكن بضغطة واحدة على لوحة المفاتيح أن تنتقل ملايين الدولارات من مكان إلى آخر، كما أنها تتميز بأنها جرائم فى الخفاء يصعب إثباتها لغياب الدليل المادى، وكذلك يطلق عليها الجرائم الناعمة حيث لا تتطلب استخدام العنف، فاتلاف بيانات فى الحاسوب أو نقلها من مكان إلى آخر لا يتطلب اى كسر أو حرق مثلا.

ويمكن القول أيضا أن التاثيرات الإقتصادية لهذه الجرائم خطيرة جداً حيث يلحق خسائر فادحة بالمجتمع.

ونوجز بعض الخصائص فى النقاط التالية:

أولا: مقترفى جرائم الحاسوب:

قد يكون مقترف هذه الجريمة شخصاً عاديا يعمل لحسابه أو الآخرين، وقد يهدف إلى تحقيق مصلحة خاصة من وراء الجريمة التى يرتبكها ضد أحد نظم المعالجة الآلية للبيانات والمعلومات [٢٠].

[٢٠]- أنظر: د/ احمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلى (الحماية الجنائية

ثانيا: الهدف والدافع من إقتراف جرائم الحاسوب:

الهدف الغالب على هذه الجرائم هو إدخال تعديل على عناصر الذمة المالية، ويكون الطمع الذى يشبعه الاستيلاء على المال دافعها، وبريق المكسب السريع محرك لمرتكبها، وقد ترتكب أحياناً لمجرد قهر نظام الحاسب الآلى وتخطى حواجز الحماية المقامة حوله أو بدافع الإنتقام من رب العمل أو أحد الزملاء أو الأصدقاء [٢١].

ثالثا: موضع جرائم المعلوماتية من مراحل تشغيل نظام المعالجة الآلية للبيانات:

على الرغم من إمكانية ارتكاب جرائم المعلوماتية اثناء اية مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلية للبيانات فى الحاسب الآلى (الإدخال- المعالجة- الإخراج) ، فإن لكل مرحلة من هذه المراحل نوعية خاصة من الجرائم لا يمكن لطبيعتها إرتكابها إلا فى وقت محدد يعتبر بالنسبة لمراحل التشغيل – الأمثل لذلك، ففى مرحلة الإدخال : حيث تترجم المعلومات إلى لغة مفهومة من قبل الآلة، فانه يسهل إدخال معلومات غير صحيحة وعدم إدخال وثائق أساسية، وفى هذه المرحلة يرتكب الجانب الأكبر من جرائم المعلوماتية، وفى مرحلة المعالجة الآلية للبيانات: فإنه يمكن إدخال أية تعديلات تحقق الهدف الإجرامى عن طريق التلاعب فى برامج الحاسب الآلى (مثل دس تعليمات غير مصرح بها فيها، أو تشغيل برامج جديدة تلغى- جزئياً أو كلياً – عمل البرامج الأصلية) ، والجرائم المرتكبة فى هذه المرحلة تتطلب توافر معرفة فنية عميقة لدى الجانى، واكتشافها صعب، وغالبا ما تقف المصادفة وراءة، وفى هذه المرحلة الأخيرة المتعلقة بالمخرجات يقع التلاعب فى النتائج التى يخرجها الحاسب بشأن بيانات صحيحة أدخلت فيه وعالجها بطريقة صحيحة [٢٢].

رابعاً: التعاون والتواطؤ على الاضرار:

وهو أكثر تكراراً فى جرائم المعلوماتية عنه فى الانماط الأخرى لجرائم

للحاسب الآلى) – دراسة مقارنة- دار النهضة العربية، القاهرة، ٢٠٠٠، ص ١٦٧

[٢١]- أنظر: د/ هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات مكتبة الآلات الحديثة، أسيوط ، ١٩٩٢ صفحة ٣٨.

[٢٢]- أنظر: د/ هشام محمد فريد ، المرجع السابق، ص ٣٩ .

الخاصة أو جرائم أصحاب الياقات البيضاء، وغالبا ما يكون متضامنا فيها متخصص فى الحاسبات الآلية يقوم بالجانب الفنى من المشروع الإجرامى ، وشخص آخر من المحيط أو من خارج المؤسسة المجنى عليها لتغطية عملية التلاعب وتحويل المكاسب اليه، كما أن من خصائص من يمارسون التلصص على الحاسبات تبادل المعلومات بصفة منتظمة حول أنشطتهم [٢٣].

[٢٣]- أنظر: د/ هشام محمد فريد ، المرجع السابق، ص ٤٠.

خامسا: دور المخالطة الفارقة:

تتجلى فى الجرائم المعلوماتية أعراض المخالطة الفارقة The differential association syndrome بشكل ملحوظ، نظراً لانتشار أنواع خاصة من الممارسات والعمليات غير المشروعة فى ميادين استخدام المعالجة الآلية للبيانات والمعلومات، واعتبار بعضها من قبيل الانحراف المقبول فى هذه الميادين، مما يتيح وييسر اقدام العاملين فيها على ارتكاب أفعال غير مشروعه قد تصل إلى حد الجرائم الخطيرة، أضف إلى ذلك أن الطبيعة التنافسية لعمل المتخصيصن فى مجال الحاسبات الآلية ومراكزهم المرموقة – غالبا- يمكن أن تؤدى إلى نوع من الإثارة والتزاحم بينهم فى ارتكاب جرائم المعلوماتية[٢٤].

سادسا: أعراض النخبة:

يعتقد بعض المتخصصين فى تقنية الحاسبات والمعلوماتية أن من مزايا مراكزهم الوظيفية ومهاراتهم الفنية استخدام الحاسبات الآلية وبرامجها وتقنياتها لأغراض شخصية، أو للتبارى الفكرى فيما بينهم، أو ممارسة بعض الهوايات الدائرة فى فلك هذه التقنية ، وهو ما يعبر عنه بأعراض النخبة syndrome elitiste، وقد يدفع ذلك بعضهم إلى التمادى فى استخدام نظم الحاسب الآلى بطريقة غير مشروعة قد تصل إلى حد ارتكاب الجرائم الخطرة[٢٥].

سابعاً : اضرار جرائم المعلوماتية:

تقع جرائم المعلوماتية وترتكب فى اطار تقنية وتكنولوجيا متقدمة يتزايد استخدامها يوما بعد يوم فى إدارة مختلف المعاملات الإقتصادية والمالية والخدمية – الوطنية والدولية على حد سواء – ويعتمد عليها فى تسيير معظم شئون الحياة اليومية للافراد والشئون العامة لاكثر الحكومات بما فى ذلك الأمن والدفاع، ومن شأن ذلك أن يضفى أبعادا خطيرة غير مسبوقة على حجم الأضرار والخسائر التى تنجم عن ارتكاب هذه الجرائم على مختلف القطاعات والمعاملات، ولا أدل على ذلك من أن حجم الخسائر المادية الناجمة عن هذه الجرائم قد بلغ وفقا لتقديرات المركز الوطنى لجرائم الحاسب فى الولايات المتحدة الأمريكية

---

[٢٤]- أنظر: د/ هشام محمد فريد ، المرجع السابق، ص ٤٠.

[٢٥]- أنظر: د/ هشام محمد فريد ، المرجع السابق، ص ٤٠.

(NCCCD) حوالى ٥٠٠ مليون دولار امريكى سنويا، بينما قدرتها مصادر أخرى بما يتراوح بين ٣ و ٥ بليون دولار فى السنة[٢٦] ، ولا شك أن هذه الخسائر قد فاقت بكثير تلك الأرقام فى عرصنا الحالى.

[٢٦]- أنظر: د/ هشام محمد فريد ، المرجع السابق، ص ٤٠، ٤١ .

ثامناً: صعوبة اكتشاف جرائم المعلوماتية وإثباتها:

لا تحتاج جرائم المعلوماتية إلى أى عنف، أو سفك للدماء أو آثار اقتحام لسرقة الاموال،وانما هى أرقام وبيانات تتغير أو تمحى تماما من السجلات المخزونة فى ذاكرة الحاسبات الآلية، ولأن هذه الجرائم فى أغلب الأحيان لا تترك أى اثر خارجى مرئى لها، فانها تكون صعبة فى الإثبات. ومما يزيد من صعوبة إثبات هذه الجرائم أيضا ، ارتكابها عادة فى الخفاء، وعدم وجود اى أثر كتابى لما يجرى خلال تنفيذها من عمليات أو أفعال اجرامية، حيث يتم بالنبضات الالكترونية نقل المعلومات ، كما أن هذه الجرائم ترتكب غالبا وبصورة منظمة على صعيد أكثر من دولة باستخدام شبكات الإتصالات والمعلومات (الإنترنت)، ودون تحمل عناء الانتقال، اضف إلى ذلك إحجام مجتمع الاعمال عن الإبلاغ عنها تجنبا للاساءة إلى السمعة وهز الثقة فى كفاءة المنظمات والمؤسسات المجنى عليها، فضلا عن امكانية تدمير المعلومات التى يمكن ان تستخدم كدليل فى الإثبات فى مدة قد تقل عن الثانية الزمنية[٢٧] .

وهناك صعوبات أخرى أيضا فى إثبات هذه الجرائم تكمن – كما سبق ان بينا- فى الجناه مرتكبى تلك الجرائم الذين يتسمون بالذكاء والدهاء والخبرة التقنية أثناء ارتكابها، إضافة إلى عدم ملاءمة الأدلة التقليدية فى القانون الجنائى فى إثباتها، ومن ثم يلزم البحث عن ادلة جديدة حديثة ناتجة من ذات الحاسب، ومن هنا تبدا صعوبة البحث عن الدليل، وجمع هذا الدليل وتبدا مشكلات قبوله أن وجد، ومدى موثوقيته أو مصداقيته على إثبات وقائع الجريمة[٢٨] .

تاسعا: السمات العامة للمتورطين فى الانحراف المعلوماتى:

" تتوافر لدى الجناة مرتكبى جرائم المعلوماتية أو معظمهم مجموعة من السمات أو الخصائص التى تميزهم عن غيرهم من الجناة أو المتورطين فى أشكال الإنحراف والإجرام الأخرى، ولعل من أبرز هذه السمات ما يلى":

أ- السن: تتراوح أعمار مقترفى جرائم المعلوماتية عادة بين ١٨ و ٤٦ سنة، والمتوسط العمرى لهم ٢٥ سنه.

ب- التكوين والمعارف والعمل: ينتمى مرتكبو هذه الجرائم عادة إلى الطبقة المتعلمة، ومعظمم يكونون من العاملين بنفس الجهة أو المؤسسة المجنى

---

[٢٧]- أنظر: د/ هشام محمد فريد ، المرجع السابق، ص ٤١ ، ٤٢.

[٢٨]- أنظر: د/ هشام محمد فريد ، المرجع السابق، ص ١١، ١٢.

عليها، وهم أشخاص محل ثقة، ولا تشوب سمعتهم أو نزاهتهم شائبة، والذى يغريهم على ارتكاب جرائمهم شعورهم بالأمن نتيجة جهل تلك الجهة أو المؤسسة وكبار مديريها بعلوم وتكنولوجيا وتقنيات الحاسبات الآلية وعلوم وفنون البرمجة، فيتملكهم الشعور بامكانية ارتكاب الجريمة دون أن يتم اكتشافها.

ج- تمثلهم صورة وخصائص روبن هود (أعراض روبن هود Robin Hood syndrome) : حيث يفرق معظم مرتبكى جرائم المعلوماتية – لا سيما الهواة منهم – تفرقة واضحة بين الاضرار بالاشخاص العاديين – الذى يعتبرونه غاية فى اللا أخلاقية- والإضرار بمؤسسة أو جهة فى استطاعتها اقتصادياً تحمل نتائج تلاعبهم ، وهو ما لا يجدون غضاضة فى تقبلة.

د- خشية الضبط وإفتضاح الأمر: لما يترتب على ذلك من ارتباك مالى وفقد للمركز والمكانة.

هـ ارتفاع مستوى الذكاء [٢٩] .

السمات المميزة لجرائم الكمبيوتر والإنترنت عن غيرها من الجرائم

* جرائم الكمبيوتر والإنترنت طائفة من الجرائم التى تتسم بسمات مخصوصة عن غيرها من الجرائم، فهى تستهدف معنويات وليست ماديات محسوسة ، وتثير فى هذا النطاق مشكلات الاعتراف بحماية المال المعلوماتى أن جاز التعبير.
* كما أنها تتسم بالخطورة البالغة نظرا لأغراضها المتعددة. ونظرا لحجم الخسائر الناجم عنها قياسا بالجرائم التقليدية. ونظرا لارتكابها من بين فئات متعددة تجعل من التنبؤ بالمشتبة بهم امرا صعبا. ونظرا لانها بذاتها تنطوى على سلوكيات غير مالوفة، وبما اتاحته من تسهيل ارتكاب الجرائم الاخرى تمثل ايجاد وسائل تجعل ملاحقة الجرائم التقليدية امرا صعاب متى ما ارتكبت باستخدام الكمبيوتر .

* وتحقيق وتحرى جرائم الكمبيوتر والإنترنت والمقاضاة فى نطاقها تنطوى على

[٢٩]- أنظر: د/ هشام محمد فريد ، المرجع السابق، ص ٤٢، ٤٣.

مشكلات وتحديات ادارية وقانونية تتصل ابتداء بمعيقات ومتطلبات عمليات ملاحقة الجناة، فان تحققت مكنة الملاحقة اصبحت الإدانة صعبة لسهولة اتلاف الادلة من قبل الجناة أو لصعوبة الوصول إلى الادلة أو لغياب الاعتراف القانونى بطبيعة الادلة المتعلقة بهذه الجرائم. ونظرا لانها جرائم لا تحدها حدود وتعد من الجرائم العابرة للحدود. فتثير لذلك تحديات ومعيقات فى حقل الاختصاص القضائى والقانون الواجب التطبيق ومتطلبات التحقيق والملاحقة والضبط والتفتيش.

إن جرائم الكمبيوتر قد ترتكب عن طريق حاسب آلى فى دولة ما. فى حين يتحقق الفعل الاجرامى فى دولة اخرى فجرائم الكمبيوتر والإنترنت، لا تحدها حدود ولا تعترف ابتداء- فى هذه المرحلة من تطورها بسبب شبكات المعلومات- بعنصر المكان أو حدود الجغرافيا وتتميز بالتباعد الجغرافى بين الفاعل والمجنى عليه، ومن الوجهة التقنية، بين الحاسوب اداة الجريمة، وبين المعطيات اوالبيانات محل الجريمة فى نظام الحاسوب المستهدفة بالاعتداء، هذا التباعد قد يكون ضمن دائرة الحدود الوطنية للدولة، لكنه، وبفعل سيادة تقنيات شبكات النظم والمعلومات، امتد خارج هذه الحدود- دون تغيير فى الاحتياجات التقنية – ليطال دولة اخرى يتواجد فيها نظام الحاسوب المخزنة فيه المعطيات محل الاعتداء.

والحقيقة ان مسالة التباعد الجغرافى بين الفعل وتحقق النتيجة من أكثر المسائل التى تثير اشكالات فى مجال جرائم الحاسوب وبشكل خاص الاجراءات الجنائية والاختصاص والقانون الواجب التطبيق. وهذا بدوره عامل رئيسى فى نماء دعوات تظافر الجهود الدولية لمكافحة هذه الجرائم، ولعل هذه السمة تذكرنا بارهاصات جرائم المخدرات والاتجار بالرقيق وغيرها من الجرائم التى وقف تباين الدول واختلاف مستويات الحماية الجنائية فيها حائلا دون نجاح أساليب مكافحتها، فلم يكن من بد غير الدخول فى سلسلة اتفاقيات ومعاهدات دولية لمكافحة هذه الجرائم، وذات الامر يقال الان بشأن انشطة غسل الأموال ، وهى فى ذات الوقت الاسباب ذاتها التى تجعل موضوع جرائم الارهاب والجرائم المنظمة والجرائم الاقتصاية المواضيع الرئيسية على أجندة اهتمام المجتمع الدولى.

ولمواجهة مثل هذه الجريمة (جريمة الحاسوب) العابرة للحدود مواجهة فعالة، يجب تجريم صورها فى القانون الوطنى للمعاقبة عليها، وان يكون هناك تعاون وتضامن دولى لمواجهة مشاكلها، من حيث مكان وقوعها واختصاص المحاكم بها وجمع المعلومات والتحريات عنها والتنسيق بين الدول فى المعاقبة عليها وتحديد صورها وقواعد التسليم فيها وايجاد الحلول لمشكلاتها الأساسية وأبرزها:

١- غياب مفهوم عام متفق عليه بين الدول – حتى الآن- حول نماذج النشاط المكون للجريمة المتعلقة بالكمبيوتر والإنترنت.

٢- غياب الاتفاق حول التعريف القانونى للنشاط الاجرامى المتعلق بهذا النوع من الإجرام.

٣- نقص الخبرة لدى الشرطة وجهات الادعاء والقضاء فى هذا المجال لتمحيص عناصر الجريمة أن وجدت وجمع المعلومات والأدلة عنها للادانة فيها.

٤- عدم كفاءة وملاءمة السلطات التى ينص عليها القانون بالنسبة للتحرى واختراق نظم الكمبيوتر، لأنها عادة متعلقة بالضبط والتحرى بالنسبة لوقائع مادية هى الجرائم التقليدية وغير متوائمة مع غير (الماديات) كاختراق المعلومات المبرمجة وتغييرها فى الكمبيوتر.

٥- عدم التناسب بين قوانين الإجراءات الجنائية للدول المختلفة فيما يتعلق بالتحرى فى الجرائم المتعلقة بالحاسوب.

٦- السمة الغالبة للكثير من جرائم الكمبيوتر هى أنها- كما أوضحنا اعلاه – من النوع العابر للحدود Transnational وبالتالى تثير من المشاكل ما تثيره امثال تلك الجرائم كجرائم الاتجار بالمخدرات والاتجار غير المشروع فى الاسلحة والإتجار فى الرقيق الأبيض والجرائم الإقتصادية والمالية وجرائم التلوث البيئى.

٧- عدم وجود معاهدات للتسليم أو للمعاونة الثنائية أو الجماعية بين الدول تسمح بالتعاون الدولى أو عدم كفايتها أن كانت موجودة لمواجهة المتطلبات الخاصة لجرائم الكمبيوتر وديناميةالتحريات فيها وكفالة السرعة بها". ويمثل مشروع الاتفاقيات الاوروبية لجرائم الكمبيوتر فى الوقت الحاضر المشروع الاكثر نضجا لمواجهة جرائم الكمبيوتر بل وواحدا من اهم ادوات التعاون الدولى فى هذا المجال.

الفصل الثالث
تقسيم جرائم المعلوماتية

نتناول هذا الفصل على مبحثين على النحو التالى:

المبحث الأول : الجرائم التى تقع على الحاسب الآلى ومكوناته.
المبحث الثانى : الجرائم التى ترتكب بواسطة الحاسب الآلى ومكوناته.

المبحث الأول
الجرائم التى تقع على الحاسب الآلى ومكوناته

نتناول هذا المبحث من خلال ست مطالب على النحو التالى:

المطلب الأول : سرقة البرامج والمعلومات المخزنة آلياً.
المطلب الثانى : سرقة منفعة الحاسب الآلى أو الاستعمال غير المصرح به لنظام الحاسب الآلى.
المطلب الثالث : بعض أفعال تزوير المعلومات والبيانات والبرامج المخزنة آلياً والتلاعب بها.
المطلب الرابع : إختراق الحاسب الآلى وإنتحال هوية المستخدم.
المطلب الخامس : التجسس المعلوماتى
المطلب السادس : الإتلاف المعلوماتى

المطلب الأول

سرقة البرامج والمعلومات المخزنة آلياً.

المقصود بسرقة البرامج والمعلومات المخزنة آلياً:

تعرف السرقة فى مفهومها العام أو الواسع بانها: " الحصول على شئ من طرف آخر بدون علم منه، وفى الغالب فإنه سيترتب عليه اضرار بهذا الطرف الآخر، سواء كان هذا الضرر مادياً أو معنوياً أو أدبياً" ، ويمكن أن يشتق من هذا التعريف الموسع لمفهوم السرقة نوعان آخران من الأفعال غير المشروعة، وهما:

أ- التجسس: وهو الحصول على معلومات بدون علم صاحب الشأن وذلك للاستفادة من هذه المعلومات بطريقة ما، أو لإلحاق ضرر بصاحب الشأن.

ب- الاحتيال: وهو إعطاء الغير معلومات غير صحيحة بهدف التضلل، أو الحصول على معلومات أو أقوال بالادعاء بما هو غير صحيح [٣٠].

أما بالنسبة لتزييف الفقة للسرقة، فقد جرى تعريفها على انه: "اختلاس مال منقول مملوك للغير بغير تملكه"، كما يعرف السارق- حسب التعريف المقنن له – بأنه :" كل من اختلس منقولا مملوكا لغيره" (المادة ٣١١ من قانون العقوبات المصرى) [٣١].

والجدير بالذكر ، فإنه فى فترة الخمسينات من القرن الماضى وحتى بداية الستينات، بدأ استخدام أجهزة الحاسب الآلى فى الانتشار على المستوى الصناعى والتجارى فى تطبيقات محدودة، وكان الهدف الاساسى من استخدامها هو إجراء العمليات الحسابية المعقدة، أو التى تتناول كما هائلاً من البيانات بسرعة وكفاءة عالية، ثم ما لبث أن صاحب هذه التكنولوجيا الحديثة اختلاف فى طريقة إجراء العمليات الحسابية وطرق تخزينها، وكذلك تقبل نوع وطبيعة الرقابة المطبقة، ومن خلال هذا الاختلاف ظهر نوع جديد من اللصوص اعتمد على تلك التكنولوجيا لتحقيق مكاسب مادية فائقة الربح، كما واكب انتشار استخدام الحاسبات الآلية على كافة المستويات وتنوع أنشطته تغيير فى النمط العام

٣٠- أنظر: د/ عثمان حجازى – السرقات والكمبيوتر- ندوة الجرائم الاقتصادية المتسحدثة – من ٢٠ إلى ٢١ أبريل ١٩٩٣ – الجزء الأول – المركز القومى للبحوث الجنائية والاجتماعية – قسم بحوث الجريمة- القاهرة ١٩٩٤- ص ٣٦٤.

٣١- أنظر د/ هشام محمد فريد رستم- ندوة الجرائم الاقتصادية، صفحة ٤٣٦، ٤٣٧.

للتعامل وإختلاف فى طريقة تناول المعلومات، ومن ذلك أخذت المعلومات فى حد ذاتها أهمية غير مسبوقة، وأصبحت المعلومة مستهدفة، وأصبح أيضا لها سوقها الخاص بها وثمنها المرتفع جدا، وترتب على ذلك فى النهاية أن أصبحت تلك المعلومات هدفاً مشتركا للسرقة فى ابسط الحالات أو للتدمير أو التجسس فى حالات اخرى، اضف إلى ذلك أن كمية الاموال المستثمرة فى تطوير برامج ونظم الحاسبات الآلية قد تعدت مئات البلايين من الدولارات، ولنا أن نتصور مدى الجاذبية لمن تسول له نفسه سرقة هذه البرامج والنظم، والخطير فى هذا الموضوع أن السرقة لم تقف عند حد الأشخاص ، بل انضمت اليهم فى ذلك مجموعة من الشركات المنظمة المنافسة، وحتى الحكومات، وذلك لسرقة المعلومات والبرامج ، وترتب على ذلك كله تطور فى اتجاه استحداث طرق جديد لحماية هذه البرامج والمعلومات [٣٢]، كما أدى هذا التطور الهائل أيضا فى تكنولوجيا صناعة برامج ونظم الحاسبات الآلية إلى تعرضها للعديد من افعال التعدى الاخرى عليها – إلى جانب السرقة- كتقليدها وإفشاء سر صنعتها، وهى تمثل ظاهرة ، وان كان لا يعرف بعد حجمه الحقيقى، إلا أنها ذات مجال واسع، ولاشك أنها تهدد – وعلى نحو مؤكد- العائد الاستثمارى لمنتجى هذه البرامج[٣٣].

وترجع البدايات الاولى لظاهرة سرقة المعلومات إلى فترة الستينات من القرن الماضى ايضا، عندما طرحت وسائل الاعلام على بساط البحث المعلومات الاولية التى تتناول ما يطلق عليه بصفة عامة" جريمة نظم المعلومات" حيث تعالج هذه المعلومات فى غالبيتها التلاعب بالحاسب الآلى وتعطيلة وسرقة المعلومات المختزنة فيه، علاوة على التجسس عليه واستخدامه على النحو غير المشروع، ونظرا لأن هذه البيانات والمعلومات قد شيدت على تقارير الصحف، فكان من الصعب جدا معرفة ما إذا كانت هذه الظواهر من وحى الخيال أم هى من قبيل الحقيقة [٣٤].

وهناك نماذج عديدة من الجرائم التى تقع على المعطيات المخزونة بالنظر إلى المصلحة المحمية قانونا، ومن تلك الجرائم ما يعد اعتداء على حقوق الملكية الفكرية عن طريق نسخ البرامج الاصلية وتسويقها أو استخدامها أو

---

[٣٢]- أنظر: د/ عثمان حجازى – المرجع السابق – صفحة ٣٦٥-٣٦٧.

[٣٣]- أنظر: د/ عبد الله حسين على محمود – سرقة المعلومات المخزنة فى الحاسب الآلى – ط٢ – دار النهضة العربية – القاهرة – ٢٠٠٢ – صفحة ٢١٠.

[٣٤]- أنظر : المرجع السابق – صفحة ٤١، ٤٢.

اعادة نشر المعلومات المسجلة دون إذن مسبق، مما يعرض الشركات المنتجة لهذه البرامج للكثير من الخسائر المادية الفادحة، وقد كشف تقرير شامل حول قرصنة برامج الكمبيوتر عن تقدير الخسائر فى هذا المجال والتى بلغت ١١.٢ مليار دولار امريكى فى عام ١٩٩٦، وهى ثانى دراسة مستقلة يتم نشرها من قبل اتحاد منتجى برامج الكمبيوتر التجارية وجمعية ناشرى برامج الكمبيوتر، وهما الجمعيتان التجاريتان الرائدتان فى مجال صناعة برامج الكمبيوتر ، وقد اشارت أيضا تلك الدراسة إلى أن من اصل ٥٢٣ مليون برنامج تطبيقى عملى جديد مستعمل عالميا فى عام ١٩٩٦ يوجد ٢٢٥ مليون برنامج غير شرعى، أى ما يوازى برنامجا من اصل اثنين هو غير شرعى، مما يشكل زيادة نسبتها ٢٠% فى عدد البرامج المقرصنة بالمقارنة مع تقديرات عام ١٩٩٥ والتى أفادت بوجود ١٨٧ مليون برنامج غير شرعى [٣٥].

وهناك العديد من صور السرقات والانتهاكات التى تقع على البرامج والمعلومات المخزنة آليا فى الحاسب الآلى ، ولعل من أهم تلك الاعتداءات غير المشروعة ما يلى:

أولا: النسخ غير المشروع للبرامج والملفات (قرصنة البرامج Software) piracy[٣٦]

---

[٣٥]- أنظر : المرجع السابق – صفحة ٢١٠.

[٣٦]- تعنى القرصنة Piracy فى مفهومها العام" كل عمل عنف غير مرخص به يرتكب بقصد النهب من قبل سفينة خاصة ضد سفينة اخرى فى أعالى البحار" وفى اللغة تطلق كلمة قرصنة على " السطو على سفن البحار" ومنذ اوائل القرن الثامن عشر صار هذا المصطلح يطلق وصفا – من باب القياس والاستهجان – على نهب المصنفات المنشورة للغير بنسخها دون ترخيص لاغراض تجارية، وطبقا لهذا المدلول شاع استخدام تعبير " قرصنة البرامج "Software piracy" وصف عملية النسخ غير المشروع لبرامج الغير، وان كان البعض يستخدم التعبير بمعنى واسع يشمل النسخ أو الاستخدام غير المرخص به للبرامج، فان آخرين يستخدمونه بمعنى نسخ البرامج المعلوماتية وتسويقها بصورة غير مشروعة، ويوسع فريق آخير من دلالة هذا التعبير بتبنيه تعريفا لقرصنة البرامج مؤداه انصرافها إلى : كل أخذ غير مصرح به أو استيلاء أو اعادة انتاج أو استخدام لبرنامج معلوماتى فى الوظيفة المعد لادائها طالما كان هذا البرنامج مقرا به، كمادة ذات قيمة، والقرصنة اذا وردت منعونة" بالمعلوماتية" كان مراداً بها نسخ البرامج بصورة غير شرعية أو الحصول على معلومات مخزنة فى ذاكرة الحاسب الآلى دون وجه حق، وتتم هذه العملية الاخيرة اما بصورة مباشرة

هيأت حرية نسخ البرامج وتداولها بعيدا عن مصدرها الأصلى بيئة صالحة لدس البرامج الطفيلية بأشكالها المختلفة من قبل المتخصصين فى هذا المجال، كذلك فقد أدت هذه الممارسات إلى حرمان العديد من الشركات المنشأة للبرامج أو الملفات- وهى صاحبة الحق فى بيع تلك البرامج – من جنى أرباح عملها(٣٧).

" ولأعمال القرصنة فى ميدان البرامج صور عديدة ومتنوعة، لعل أبرزها وأخطرها على صناعة البرامج المعلوماتية الصور الأربعة التالية:

١- تقليد البرامج Software contefeiting: ويقصد به محاكاة برنامج معين عن طريق صنع العديد من النسخ المماثلة له أو إنتاجها بحيث تبدو عند تسويقها كما لو كانت هى الأصل، والنسخ الجزئى للبرنامج كاف للقول بتقليده ما دامت المحاكاة تتعلق باجزائة الرئيسية، والتقليد- كصورة من صور القرصنة- يهدد برامج الألعاب الإلكترونية بصفة خاصة، فضلا عن كونه احد ابرز المشكلات التى تواجه منتجى البرامج العامة ، ونظرا لضخامة الارباح التى تجنى من وراء هذا التقليد، وتدنى مخاطرة المحتملة، وصعوبة اثباته على الواقع العملى الملموس، فقد ادى ذلك إلى اعتباره– وبحق – من أبرز مجالات الانشطة غير المشروعة التى تجذب المتورطين فى الجريمة المنظمة.

٢- سرقة البرنامج المصدر Source program:،وازالة ما يميز هويته بادخال تغييرات على شكلة وهيئته ، واعادة تجهيزه ليبدو كما لو كان منتجا جديداً لصانع آخر، واكثر المهددين بخطر هذا النمط من القرصنة هم منتجى حزم البرامج الجاهزة التى جرى تسويقها على نطاق واسع، ومن المتوقع

عن طريق الحصول على كلمة السر سواء بالحيلة أو باجراء تجارب مع الكلمات التى تستعمل لهذا الغرض عادة، واما بصورة غير مباشرةعن طريق التقاط الموجات الكهرومغناطيسية المنبعثة من الحاسب اثناء تشغيلة وترجمتها ، ولا تختلط القرصنة وفقا لذلك بما يسمى" فيروس الحاسب " وان كان ممكنا الجمع بين الافتين، " كما لو عد قرصان الحاسب إلى زرع فيروس عندما يشعر انه على وشك ان يكشف امره).

د/ هشام محمد فريد رستم- قانون العقوبات ومخاطر تقنية المعلومات ، المرجع السابق، ص ١٠٤-١٠٧.

٣٧- أنظر: د/ هدى صلاح – الجريمة فى مجال نظم المعلومات – ندوة الجرائم الاقتصادية المستحدثة- المركز القومى للبحوث الجنائية والاجتماعية – القاهرة – ١٩٩٤، صفحة ٣٥٨.

تفاقم حدة هذا الخطر كلما تزايدت بين هؤلاء المنتجين حدة المنافسة.

٣- النسخ المباشر Straight forward copying للبرامج وبيعها دون دفع مقابل مالى للحصول على ترخيص بذلك من منتجيها أو سداد انصبة فى العائدات الناتجة عن بيعها، وتعد انظمة التشغيل المعقدة أو المتقدمة sophistiated operating systems للحسابات المتوسطة Mini computer اضافة إلى برامج الخدمات " المساعدة" وبرامج الترجمة Utility and Compilers programs، من أكثر المجالات التى يمارس فيها هذا النمط من القرصنة .

٤- النسخ غير المشروع للبرامج دخل المنظمات والشركات الكبيرة عند الحصول على منتجيها على ترخيص نسخها مرة واحدة، فيتم نسخها بصورة غير قانونية مرات متتالية،وتشيع ممارسة هذا النمط من القرصنة فى معظم الشركات والمؤسسات، وتزداد حدته بشكل خاص فى قطاع تسويق برامج الحاسب الشخصى Personnel computer[٣٨].

أساليب ارتكاب افعال قرصنة البرامج والملفات:

تتنوع أيضا أساليب ارتكاب عمليات القرصنة التى يكون محلها برمجيات ونظم الحاسبات الالية، وتنقسم تلك الأساليب إلى أساليب تقليدية واخرى فنية:

١- الأساليب التقليدية:

ومن صور تلك الأساليب رشوة أو ابتزاز الموظفين العاملين فى شركات إنتاج برمجيات الحاسبات الالية، وتسلل الموظفين إلى الشركات المراد التجسس على برامجه للعمل فيها فترة وجيزة تسمح لهم بالاطلاع على أسرار ودقائق برامجها، أو الإعلام عن وظائف وإجراء مقابلات مع المتقدمين لشغلها للحصول منهم على وصف لأعمالهم اوعمليات الشركات التى ينتمون اليها، ويقدر البعض أن ٦٣% من عمليات سرقة البرامج ترتكب عن طريق الموظفين العاملين فى شركات انتاج البرامج الذين ينقلون البرامج الجديدة فى حقائب اوراقهم ويغادرون مكاتبهم رأسا إلى القراصنة[٣٩].

٢- الأساليب الفنية:

" تفيد الخبرات المستمدة من بعض علميات قرصنة برامج الحاسب

---

[٣٨]- أنظر : د/ هشام محمد فريد رستم، المرجع السابق ص ١١١، ١١٦.

[٣٩]- أنظر : د/ هشام محمد فريد رستم ، ص ١٢٦.

الآلى التى تم اكتشافها انه عندما تتوافر لدى أى شخص امكانية الإتصال المنطقى بالحاسب Logical access فان خطر الوصول إلى برامجه والحصول على نسخ منها يصبح قائما، ومن الحالات التى تشهد بتحقق هذا الخطر فعليا حالة لشاب يبلغ من العمر أربعة وعشرين عاما تمكن – باستخدام احدى خطوط الإتصال الهاتفى- من الدخول عن بعد إلى انظمة احدى مراكز الحاسبات وسرقة" نسخ " برنامج يخصه قيمته مليون دولار، وفى حالة اخرى تمكن مبرمج باحدى الشركات بمدينة بالو آلتو Palo Alto ، بولاية كاليفورنيا الأمريكية من الوصول عن بعد إلى ذاكرة الحاسب الالكترونى لشركة منافسة وطبع برامج معلوماتى معين يخص الشركة الاخيرة تبلغ قيمته ٣٠٠ الف دولار، وكانت مؤسسته قد لاحظت أن عدم استخدامه فى اعمالها الهندسية قد سبب انخفاضا فى مبيعاتها.

ويشير البعض إلى امكانية الحصول على نسخ من البرامج باستخدام شاشات التسجيل عن بعد وادوات المراقبة السمعية، ففى احدى حالات القرصنة كانت الوسيلة المستخدمة هى التقاط وتسجيل موجات البرامج المعلوماتية التى يجرى بثها عبر الأثير(٤٠).

ومع أن منتجى البرامج يبذلون قصارى جهدهم لتزويدها بوسائل فنية تحميها من خطر النسخ غير المرخص به، الا أن جهدا مضادا لا يكف القراصنة

٤٠- فى تلك الحالة تلقت شركة A & F لانتاج وبث البرامج المعلوماتية بانجلترا بلاغا من مجهول يفيد أن بعض مشغلى اجهزة الاستقبال والارسال اللاسلكية يتبادلون فيما بينهم بث برامج الشركة لتسجيلها دون دفع الرسوم المقررة للحصول من الشركة على ترخيص بذلك، وللتحقق من صحة تلك الواقعة، قامت الشركة المذكورة بشراء جهاز استقبال للموجات اللاسلكية واستخدامه فى مراقبة الموجات الحاملة للبرامج عبر الاثير، وسرعان ما اكتشفت أن ثلاثة من برامجها يجرى بثها بانتظام كى تسجل مجانا من قبل اخرين، وان واحدا ممن يقومون بذلك يبث بانتظام قائمة تحتوى على اكثر من ٤٠٠ برنامج، وكشفت اجهزة الرصد والمتابعة أن عمليات بث البرامج تغطى مساحات شاسعة من الولايات المتحدة، وقد قدرت الشركة حجم الخسائر الناجمة عن نقص مبيعات برامجها بسبب هذه القرصنة بمبلغ ٧٥ الف جنيه استرلينى فى السنة، ومع ذلك فان تلك الشركة لم تتخذ ايه اجراءات فعالة لملاحقة هؤلاء القراصنة قضائيا، واكتفت بالحصول من بعضهم – بعد التوصل اليهم – على تعهد بعدم تكرار ذلك مستقبلا تقديرا منها لعدم علمهم باحكام القانون التى تحظر هذا البث والتسجيل، واخذا فى الاعتبار أن ما قاموا به لم يتعد مجرد تبادل البرامج بين الاصدقاء.
د/ هشام محمد فريد رستم ، هامش (٣) ، ص ١٢٨- ١٢٩

عن بذلة لفك رموز البرامج المسروقة،وزيادة قدرات برامج النسخ للتغلب على وسائل الحماية الفنية التى تزود بها البرامج المستنسخة ، ولا ادل على هذا الجهد من أن أى صبى صغير متمرس بالحاسب- كما يقول Michael Crichton- سيجيب إذا ما سئل عما إذا كان نسخ البرامج ممكنا، بان كل شئ يمكن نسخة ، والمعنى ذاته يؤكده البعض بقوله أن الطرق الفنية لجعل نسخ البرامج مستعصيا هى الاسهل فى الاستخدام لحمايتها من خطر القرصنة، والاسهل فى ذات الوقت أيضا فى امكانية تخطيها والتغلب عليها، ومن ثم نسخ وسرقة تلك البرامج ، ايه ذلك أن البرامج المخصصة لنسخ البرامج المحمية فنيا ضد خطر النسخ تنسح هى الاخرى بدوها [٤١]،[٤٢].

ثانيا: النسخ غير المشروع البيانات المخزنة الكترونيا

وتعتبر هذه الصورة أيضا نوعا من انواع القرصنة المعلوماتية، حيث تخزن البيانات والمعلومات المعالجة الكترونيا على هيئة نبضات كهربائية فى دوائر مجمعة أو على اشرطة واسطوانات ممغنطة، وفى الحالتين يمكن نسخها على دعامات اخرى معينة [٤٣]، ومن اشهر الامثلة على ذلك ما حدث لأكبر شركة امريكية متخصصة فى توفير خدمات الانترنت فى عام ٢٠٠١ – والتى تخدم أكثر من ٢٣ مليون مستخدم للإنترنت – عندما قام شاب يبلغ من العمر تسعة عشر عاما يدعى " جاى ساتيرو" باقناع مسئوليها بانه مفيد للشركة، فقاموا بتعينه على الفور، وعنما اظهر مهارة فى العمل، طوال سنتين متواصلتين يجمع معلومات سرية مهمة عن الشركة ، وفجاة قرر الاستقالة بحجة الحصول على وظيفة اخرى، لكنه فى الحقيقة كان يجهز لاستخدام ما جمعه من بيانات فى شن

---

[٤١]- وتاكيدا لسهولة نسخ البرامج يقرر الدوريسيت – احد القراصنة فى مجال سرقة البرمجيات الفرنسيين المهرة- ان اكثر من ٩٠% من البرامج لا تحتاج لاكثر من خمس دقائق لنسخها، وان كان بعض المعقد من تلك البرامج قد يتطلب عمل اسبوعين متواصلين لنسخة، والواقع ان الوسائل الفنية التى تزود بها البرامج لحمايتها من خطر النسخ غير المرخص، به ستعوق فحسب – كما قيل – المستخدمين الشرعيين الذين هم فى حاجة لعمل نسخ احتياطية، اما القراصنة فسيمكنهم الاستمرار فى نسخ البرامج نظرا لما يتمتعون به من مهارات تقنية تتيح لهم التغلب على ما تزود به البرامج من وسائل فنية.

د/ هشام محمد فريد رستم ، هامش (١) ، ص ١٢٩

[٤٢]- د/ هشام محمد فريد رستم ، ص ١٢٧- ١٢٩

[٤٣]- د/ هشام محمد فريد رستم ، ص ٢٣٥

هجمات شديدة القسوة على موقع الشركة ، وبعد فترة من استقالته لاحظ المسئولين عن تامين موقع الشركة ان هناك شخصا يهاجم الموقع بإحتراف شديد، تنهار امامه جميع اجراءات التامين ويخترقها بسرعة، ثم يقوم باستبدال البرامج الخاصة بالموقع ببرامج اخرى من عنده تعطل العمل وتسبب مضايقات عديدة للعاملين فى الشركة، وبعد فترة طور هذا القرصان من عملياته وبدا يسرق الارصدة المدفوعة من اشتراكات الخدمات ، وقد كلفت هذه العمليات غير المشروعة الشركة ٥٠ ألف دولار خلال وقت قصير جدا[٤٤].

ثالثا: الجرائم الالكترونية:

ذكرنا ان الجرائم الالكترونية هى نوع من انواع جرائم المعلوماتية، تتمثل فى استخدام برامج الحاسب الآلى ونظمه لالتقاط بيانات ومعلومات معالجة الكترونيا والتلاعب بانظمة الحاسبات التى تحتوى عليها، وذلك لاغراض غير مشروعة- تتمثل غالبا فى السرقة والاحتيال- وباستخدام هذه البرامج والتعرف على نقاط الضعف فى نظام الحاسب الآلى الخاص بالمجنى عليه، فان الجانى يستطيع أن يسيطر على نظام هذا الحاسب باكمله، ثم يقوم بنشاطه غير المشروع ، ويحول هذا النشاط فى النهاية إلى مكاسب غير مشروعه، وينتهى بمحو كل اثر يمكن أن يكشف عن افعاله الإجرامية.

ولعل خير مثال يمكن أن يوضح ميكانيزم الجريمة الالكترونية، ما قام به احد الجناة الالكترونيين فى الولايات المتحدة الأمريكية ويدعى" آلان كيدمان" فعلى الرغم من صغر سنة- الذى لم يتجاوز العشرين عاما- فانه قام بارتكاب العديد من الجرائم الالكترونية المحنكة فى الفترة من سنه ١٩٩٨ وحتى عام ٢٠٠٢، حيث تم التاكد من تورطه فى مجموعة هجمات الكترونية شنها على أجهزة كمبيوتر حساسة خاصة بوكالة الفضاء الأمريكية "ناسا" نتج عنها بعض الخلل فى انشطة تلك الوكالة، وكان هذا الجانى يركز على الأجهزة المحملة ببرامج علمية مسئولة عن تطوير نظم اطلاق الاقمار الصناعية، وبالتالى اصبح بامكانية تدمير البيانات المسجلة على قواعد أو تغييرها ببيانات اخرى تؤثر على دقة وسلامة انطلاق الاقمار الصناعية، مما كان سيؤدى إلى حدوث العديد من الكوارث الدولية، كما كان يقوم بكسر كلمات السر وحواجز المرور ودس العديد

[٤٤]- مجلة الأهرام للكمبيوتر والإنترنت والاتصالات " لغة العصر" ، العدد التاسع عشر، يوليو ٢٠٠٢، ص ٨٠- ٨١.

من البرامج غير الشرعية التى تستطيع اجبار أجهزة الكمبيوتر على تنفيذ الاوامر دون تمريرها على الانظمة الامنية الالكترونية، ولم يكتف هذا القرصان بجرائم الاختراق الالكترونى ومهاجمة أجهزة الكمبيوتر وقواعد البيانات الخاصة بالجامعات ووكالة الفضاء الأمريكية "ناسا" بل حاول توسيع نشاطه بعد أن اكتشف انه يمتلك موهبة اجرامية تمكنه من بدء رحلة المليون بسهولة وفى زمن قياسى بدلا من الاكتفاء بتدمير الأجهزة دون سبب واضح ودون مكاسب مالية، فبدأ فى استخدام البرنامج الخاص بالتجسس على المواقع التجارية على الانترنت لتسجيل كلمات المرور واسماء المستخدمين الخاصة بكروت الائتمان التى يتم التعامل بها مع المواقع التجارية، وعن طريق استخدام كلمة المرور قام "كيدمان" بثلاث محاولات لتحويل الاموال الخاصة باصحاب كروت الائتمان لحسابه الخاص فى البنك، وبعد محاولتين منهما فاشلتين نجح فى الثالثة فى سحب مبلغ كبير من المال عن طريق ارقام مسروقة لكارت ائتمان، لكنه لم يتمكن من تحويلها لحسابه الخاص نظرا لاكتشاف خطا رقمى ارتكبة هذا القرصان لحداثته فى هذا المجال، وهكذا تم ابلاغ الجهات الامنية فى الولايات المتحدة الأمريكية لمراقبته وتعقبة واثبات العديد من الافعال الجنائية التى قام بارتكابها[٤٥].

رابعا: السطو المسلح الالكترونى:

ادى التطور المستمر لاستخدام المعلوماتية إلى التزايد الحتمى للمعالجات والتخزينات ، ومن ثم زيادة تدفق المعلومات فى شكل ممغنط أو الكترونى بدلا من الشكل الكتابى، كما ترتب على ظهور التقنيات المستحدثة – اى تقنيات بث المعلومات على شبكة اتصالات بعدية **Télématique** والمعالجة عن بعد **Télétraitement** – نشوء مخاطر جديدة نتيجة للامكانيات المستحدثة للولوج والاستفسار عن بعد من المراكز المعلوماتية، وتشكل عمليات البث **Transmission** أيضا نقطة ضعف هامة فى النظام المعلوماتى.

ويمكن أن نصادف المشاكل المرتبطة باستخدام انظمة المعالجات عن بعد وشبكات البث فى مراحل عديدة ومختلفة لاستعمال الاساليب الالكترونية، وفى الواقع، فان المعلومات اثناء حركتها وبثها، تكون مهددة فى كل لحظة بالالتقاط

[٤٥]- مجلة الأهرام للكمبيوتر والإنترنت والاتصالات " لغة العصر" ، العدد الثامن ، اغسطس ٢٠٠١، ص ٧٠.

أو بالتسجيل غير المشروع.

١- التقاط المعلومات المتواجدة ما بين الحاسب الآلى والنهاية الطرفية:

ويتم هذا الالتقاط عن طريق توصيل خطوط تحويله، والتى ترسل اشارات الكترونية" ذبذبات الكترونية مكبرة" تمثل المعلومات المختلسة إلى النهاية الطرفية المتجسسة، أو عن طريق مرسل صغير يسمح بنقل المعلومات عن بعد، وعلى النقيض عندما تسلك المعلومات الطريق الجوى- كما فى حالة البث عن طريق القمر الصناعى – توضع هوائيات مطاردة بالقرب من الهوائيات الاحتياطية، والتى تمسح بالتقاط الاشعاعات واحتجاز مضمونها.

٢- التوصيل المباشر على خط الكترونى Wire Tape:

وتباشر هذه التقنية عن طريق وضع مركز تنصت يسهل تسجيل كل الإتصالات، كما يمكن أن تؤدى هذه الوظيفة أيضا ميكروفونات صغيرة.

٣- التقاط الاشعاعات الصادرة عن الجهاز المعلوماتى Electromagnetic pickup

ويمكن عن طريق هذه التقنية اعادة تكوين خصائص المعلومات التى تتحرك وتنتقل من خلال نظام معلوماتى، ويكفى لاتمام ذلك أن تسجل ثم تحل شفرة الاشعاعات الالكترومغناطيسية المنبثة بواسطة أجهزة الكترونية، وفى الواقع، تصدر بعض عناصر الانظمة القوية – وعلى وجه الخصوص الطابعات السريعة Les imprimantes rapides – اثناء تادية وظيفتها اشعاعات الالكترومغناطيسية ، وقد ثبت انه بامكان شاحنة صغيرة مجهزة تجهيزا خاصا وتقف بمحازاة مبنى مكتظ بالحاسبات الآلية أن تلتقط وتسجل هذه الاشاعات، ويمكن عن طريق جهاز لفك الرموز أن يطلب من طابعة متصلة بنظيرتها الموجودة فى المركز المستهدف النسخ الحرفى لنفس هذه المعلومات، ونذكر فى هذا الخصوص مثال شهير للسطو المسلح الالكترونى، وهو خاص باختلاس اموال عن طريق التقاط امر بالتحويل مرسل من بنك إلى آخر، وقد تمكن المختلس من تزييف الرسالة بالامر بدفع نفس المبلغ لحساب فتح باسمه.

٤- التدخل غير المشروع فى نظام بواسطة طرفيه بعيدة " الولوج غير المسموح به فى نظم المعلومات " Phone Freak:

ادى ربط الحاسبات الآلية بعضها بالبعض الاخر عن طريق شبكات المعلومات إلى سرعة انتقال المعلومات من جهة، والى سهولة التطفل عليه من

جهة اخرى، ويمكن عن طريق تقنية بث المعلومات على شبكات اتصالات بعدية télématique التدخل أو الدخول فى نظام معلوماتى من بعد، ثم يصبح بعد ذلك نسخ المعلومات أو التطفل عليها أو تدميرها شيئا سهلا، ويكفى لبلوغ ذلك استخدام جهاز المودم Modem والتزود بكلمة السر أو مفتاح الشفرة المناسب، حيث يسمح هذا الجهاز للمتطفلين من اية مسافة يتواجدون فيها بالولوج من الحاسبات الآلية المستهدفه، ودون اى مساس مادى بحق ملكية الغير، أو ترك اثر يدل على انتهاك المعلومات أو نسخها[٤٦].

وقد أبانت صحيفة Canard en Chainé الفرنسية عن عملية تعدى من بعد على ذاكرات الحاسبات الآلية بالشركة الدولية للخدمات المعلوماتية C.I.S.I وهذه هى احدى الحالات النادرة التى كشف عنها فى فرنسا[٤٧].

خامسا : سرقة البرامج والمعلومات المخزنة آليا عن طريق الهاكرز والكراكرز[٤٨]:

---

[٤٦]- أنظر : د/ محمد سامى الشوا، ص ٢٠٤.

[٤٧]- أنظر : د/ محمد شامى الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات ، دار النهضة العربية، القاهرة، ١٩٩٤، صفحة ٦٨، ٧١.

[٤٨]- فى الستينات من القرن الماضى كانت كلمة هاكرز تطلق على المبرمجين الذين لهم خبرة واسعة ودراية كاملة بخبايا البرامج والنظم، وكانوا يقدمون يد العون لكل المؤسسات التى تدار بواسطة الكمبيوتر، وفى ذلك الوقت كانت لغات البرمجة السائدة هى الكوبول، والفورتان والبيزك التقليدى ، تلك اللغات التى لا يسمع عنها الان الا زوار متاحف الكمبيوتر، وحتى ذلك الوقت كانت كلمة هاكرز تطلق على المبرمجين الشرفاء ولعل اشهرهم فى تلك الفترة هما: " دنيس ريتشى وكيفين تومسون" اللذان وضعا حجر الاساس لنظام التشغيل Unix ومع بدايات ظهور نظام التشغيل Windows الذى كان يحتوى على العديد من الثغرات الامنية- ومازال ومع بداية ظهور الانترنت بدا بعض الهاكرز ياخذون منعطفاً اخر الا وهو الاختراق والتجسس على اجهزة الكمبيوتر وسرعان ما فقدت كلمة هاكرز معناها الحقيقى واصبحت تطلق على لصوص ومخترقى اجهزة الكمبيوتر بغرض سرقة المعلومات، ولعل اشهر لصوص الهاكرز على مر التاريخ والذى يطلق عليه " ملك الهاكرز " وهو " كيفين ميتنيك " الذى حطم الكثير من الدفاعات الحصينة لاجهزة الكمبيوتر للعديد من المؤسسات والهيئات ووصل إلى ادق ما تحتوى تلك الأجهزة من معلومات بدءا من شركات الاتصالات الموجودة فى محيط مدينته وصولا إلى وزارة الدفاع الامريكية " البنتاجون"

الهاكرز والكراكرز كلاهما لص معلوماتى، الا أن هناك فارقا بينهما يتمثل فى الغاية التى يسعى إليها كل منهما، فالغاية التى يسعى إليها الهاكرز هى اختراق أجهزة الحاسب الآلى للحصول على المعلومات، أما الكراكرز فهم المحطمون لكلمات السر والكاسرون لحماية برامج الحاسب الآلى، وكل ما يشغلهم هو كيفية نسخ وتداول البرامج المحمية[٤٩].

سادسا: بعض صور الاحتيال المعلوماتى التى تقع على البرامج والمعلومات المخزنة آليا:

ففى تلك الصور يقوم الجناة بالتلاعب فى نظم معالجة المعلومات للحصول بغير حق على اموال أو أصول أو خدمات، كما يتم التلاعب أيضا فى المعلومات والبيانات المعالجة آلياً بنية تحقيق ربح مادى غير مشروع.

اما بالنسبة للكراكرز فان كلمة كراكرز Crachers فى اللغة ماخوذة من الفعل Crack بمعنى كسر وتحطيم وبالفعل فان الكراكرز هم المحطمون لكلمات السر والكاسرون لحماية البرامج، وكل ما يشغلهم هو كيفية نسخ وتداول البرامج المحمية.

مهندس احمد حسن خميس ، الهاكرز والكراكرز ، دار البراء، الاسكندرية ، ٢٠٠٣، ص٦- ٧.

[٤٩]- أنظر : مهندس احمد حسن خميس، المرجع السابق ، ص ٦.

المطلب الثانى
سرقة منفعة الحاسب الآلى أو الاستعمال غير المصرح به لنظام الحاسب الآلى

يقصد بسرقة منفعة الحاسب الآلى "استخدامه لاغراض شخصية أو تجارية بدون علم مالكه أو حائزة القانونى" أو استخدام نظام الحاسب الآلى وبرامجة بغير تصريح بذلك من مالكه أو حائزة" ويعد هذا الفعل غير المشروع من أكثر الجرائم المعلوماتية تعارفا، وقد ترتكب تلك الجريمة أما بواسطة مستخدمى الشركات الخاصة أو المرافق العامة، وهناك العديد من الأمثلة التى تشير إلى حدوثها فى جميع انحاء العالم.

وتمارس سرقة منفعة الحاسب الآلى فى معظم حالاتها بغير غرض اجرامى، اى بدون تحقيق ربح أو استفادة ، حيث يلجأ إليها بعض الاشخاص – على سبيل المثال- لتحرير بطاقات مخصصة لأعمال الخير أو لنسخ العاب الفيديو أو برامج الحاسب الآلى لاستعمالهم الشخصى، الا انه فى بعض حالات سرقة منفعة الحاسب الآلى نجد أنفسنا ازاء مجموعة من المستخدمين تستغل الحاسب الآلى الخاص بالشركة أو الادارة التى تعمل بها كى تمارس فى الظلام أو الخفاء عملا على منوال عملها الاصلى، وهكذا اكتشف – على سبيل المثال- فى مدينة شيكاغو الأمريكية فريق مكون من خمسة اشخاص يعملون باحدى المراكز التعليمية بها، اقاموا بالفعل شركة حقيقية خاصة بهم لبرمجة اعمال عملائهم الخصوصيين على الحاسب الآلى التابع لمركز عملهم.

ويثير هذا الفرض من الناحية القانونية مسألتين : اولاهما:أن الجناة تمكنوا من الحصول على مزايا مالية غير مشروعة" كتوفير نفقات الاستعمال وتحقيق مكاسب مادية "، نظرا للاستعمال التجارى للحاسب الآلى التابع لمركز عملهم الاساسى، وثانيهما: الضرر الذى لحق بالمالك أو الحائز القانونى للحاسب الآلى لاسيما إذا ما كان هذا المالك أو الحائز مؤجراً للحاسب الآلى[٥٠].

٥٠- انظر د/ محمد سامى الشوا - صفحات ٢٢٠- ٢٢١- مرجع سابق.

ويدخل أيضا فى هذه الجريمة ما اصطلح على تسميتة من قبل الفقة بسرقة وقت الآلة أو وقت الحاسب الآلى ، اى" استخدام وقت الآلة أو وقت الحاسب من اجل اغراض شخصية" ، فقد يحدث عملاً- وبدلا من الابقاء على استخدام الجهاز المعلوماتى والموجود بمكان العمل لاغراض مهنية بحتة ومسموح بها – أن يتم الاستيلاء على وقت هذا الجهاز بمعرفه بعض المستخدمين غير الامناء بغية انجاز اعمال خاصة بهم وبدون علم الحائز الشرعى للنظام المعلوماتى.

وجريمة سرقة وقت الحاسب الآلى أو الآلة من الجرائم الشائعة فى العديد من مراكز الابحاث فى مختلف دول العالم، ففى فرنسا- على سبيل المثال – من السهولة بمكان أن ينتقل باحث من اجل توفير نفقات معملة إلى مركز أخر، ويستعير كلمة السر أو شفرة الوصل للولوج (الدخول) فى بنك المعلومات الخاص بهذا المركز، ويعد هذا الوقت للحاسب الآلى من الامور المكلفة جدا، وقد يتسبب محاسب غير امين فى احداث خسائر لمنشأة بأكملها – نتيجة لاقترافة هذه الجريمة- تفوق باضعاف اجور المستخدمين بها.

ويمكن أن نذكر فى هذا الخصوص واقعة اثنين من مستخدمى شركات غاز بريطانية ، قاما عن طريق اعلانات صغيرة ببيع رسومات صممت بواسطة النظام المعلوماتى الخاص بهذه الشركة، وهناك أيضا المثال الخاص بـ ٢٠٠ مستخدم الذين قاموا باستخدام الحاسب الآلى الخاص بمركز تصنيع وحماية الصواريخ النووية من اجل تخزين العاب اليانصيب والخطابات الشخصية"[٥١].

المطلب الثالث

بعض أفعال تزوير المعلومات والبيانات والبرامج المخزنة آلياً والتلاعب بها.

قد ترتكب بعض افعال التزوير المعلوماتى، والتلاعب فى البرامج أو البيانات أو المعلومات المخزنة آلياً، وذلك لاغراض غير مشروعة تتمثل غالبا فى الاضرار بالمصالح العليا للدولة، والحياة الشخصية للافراد.

[٥١]- انظر د/ محمد سامى الشوا - صفحات ٨٥، ٨٦ - المرجع السابق..

والأمثلة على ذلك كثيرة ومتنوعة، نذكر منها، قيام أحد الأشخاص فى المانيا بالتلاعب فى نتيجة اختبار الدم الذى اجرى له لقياس نسبة المواد المخدرة به بعد أن تمكن من الوصول إلى نظام الحاسب الآلى الذى يحتوى على نتيجة هذه الاختبارات، وما قام به بعض الاشخاص أيضا فى المانيا من تلاعب فى سجلات الشرطة بهدف حذف اسماء بعض الأشخاص المطلوب القبض عليهم، وما حدث فى يناير عام ١٩٧٩ عندما تعرضت احدى الطائرات التى هبطت فى مطار كنيدى بولاية نيويورك الأمريكية وعلى متنها السفير الروسى للخطر نتيجة تلاعب احد المراقبين الجويين بنظام الحاسب الآلى، وما حدث فى الشركة الأمريكية "TRW Computer Credity data" عندما تمكن ستة من العاملين بها من التلاعب فى البيانات والمعلومات الخاصة بالمركز الائتمانى للافراد الذين يرغب عملاء الشركة فى التعامل معهم، من خلال تعديل أو محو البيانات التى تظهر المركز الائتمانى السئ لصاحبها لتحل محلها بيانات جديدة تفيد تمتع صاحبها بمركز ائتمانى جيد، وذلك فى مقابل مبالغ مالية تم الاتفاق عليها، حيث قدر عدد السجلات التى تم التلاعب بها بحوالى مائة سجل، وبناء على تلك البيانات الإئتمانية التى تم ادخالها بالمحو أو بالاضافة أو بهما معا إلى نظام المعلومات الآلى الخاص بالشركة، قام العديد من عملائها بالدخول فى معاملات مالية وتجارية مع اشخاص ذوى سمعة ائتمانية سيئة.

المطلب الرابع
إختراق الحاسب الآلى وإنتحال هوية المستخدم.

من الممكن إختراق الحاسبات الآلية أو إنتحال هوية مستخدمى تلك الحاسبات أما مادياً أو الكترونيا، ويسمح الاختراق المادى بدخول الجانى إلى مناطق خاضعة للسيطرة عن طريق بوابات الكترونية أو آلية، واسلوب الاختراق الاكثر شيوعا هو أن يقف شخص غير مسموح له بالدخول امام البوابات المغلقة حاملا بين ذراعية متعلقات خاصة بالحاسبات الآلية- كالشرائط الممغنطة على سبيل المثال- أو ينتظر حتى يتقدم شخص مسموح له بالدخول ويفتح له الباب فيدخل معه فى نفس الوقت، ولذا فانه يمكن القول بان التواجد فى صالات الحاسب الآلية هو امر حتمى لارتكاب هذه الجرائم، وينطوى السلوك غير

المشروع فيها على اطلاع غير مسموح به على البيانات والمعلومات المختزنة فى نظم المعلومات ، ولهذا السلوك صور عديدة ، منها:

١- سرقة القائمة: وهى عملية مادية بحته يكتفى فيها السارق بسحب القائمة من الطابعة.

٢- الاطلاع على المعلومات : ويقصد به مطالعة ومشاهدة المعلومات التى تظهر على الحاسبات الآلية، ويتم ذلك لاغراض غير مشروعة تتمثل غالبا فى السرقة والتجسس والاحتيال.

٣- التنصت المجرد على المعلومات: ويتم ذلك عن طريق استخدام مكبرات للصوت تلتقط المعلومات والبيانات.

اما عن انتحال هوية مستخدم الحاسب الآلى ، فيقصد به " سرقة شخصية مستخدم آخر" ويتطلب الوصول إلى الحاسب الآلى أو إلى الطرفيات لانتحال هوية مستخدمى الحاسبات الآلية معرفة دقيقة فى اغلب الاحيان لمستعملى تلك الأجهزة، ويرتكز فحص الهوية ثم انتحالها على مجموعة معلومات متوافقة يستخدمه المستعمل ككلمة السر، أو اية جملة خاصة بالمستعمل، أو اية خاصية فسيولوجية خاصة به (كالبصمة الرقمية، أو اية ملامح للوجه أو هندسة الكف أو الصوت) ، بالاضافة إلى اى شئ يمتلكه المستعمل- كالبطاقة الممغنطة أو المفتاح المعدنى، فلو تمكن اى انسان من الحصول على تلك المجموعة من المعلومات المتوافقة، فانه يصبح قادرا على انتحال شخصية اى مستعمل لجهاز الحاسب الآلى، والامثلة على ذلك عديدة فقد ادعى شاب انه صحفى فى احدى المجلات واتصل بشركات اتصالات هاتفية مدعيا انه بصدد نشر مقالة عن النظام المعلوماتى المستخدم فى تلك الشركة، فدعته الشركة لزيارة مقرها ، ثم قدم له موظفيها عرضا كاملاً ومفصلا عن الأجهزة المعلوماتية وتطبيقاتها فى الشركة، فكانت النتيجة انه سرق منهم معدات تزيد قيمتها على مليون دولار امريكى[٥٢].

[٥٢]- انظر د/ عبد الله حسين على، مرجع سابق ، صفحات ٩٤- ٩٧.

المطلب الخامس
التجسس المعلوماتى

الحاسبات الآلية أصبحت الآن ضرورة فى كافة المجالات ، حيث تعهد مختلف الادارات والمؤسسات والمنظمات فى كل من القطاع الحكومى والقطاع الخاصة بمعلوماتها الاكثر سرية إلى الحسابات الالكترونية، مولية نظم تلك الحاسبات الامنية، ثقتها شبة العمياء، وجاهلة أو متناسية ان هذا الجهاز كثيرا ما بدا – وفقا لوصف البعض – كخزانة بغير ابواب[٥٣]، وقد ادى هذا الاستخدام المتزايد للحاسبات الآلية فى مختلف المجالات إلى تمركز المعلومات بدرجة كبيرة فى جميع الدول – المستخدمة لنظم المعلومات – فى تلك الأجهزة ، كما ادى تخزين هذه البيانات و المعلومات على هذا النحو – إلى سهولة التجسس على الاسر الصناعية والتجارية والمهنية والعسكرية، ومن ثم اصبحت تلك البيانات والمعلومات المخزنة آليا فى مجالات عديدة – كالابحاث والتجارة والطاقة النووية.. وغيرها – تشكل الهدف المفضل لانشطة التجسس غير المشروع، وعلى سيل المثال، فان (الحسابات، والموازنات ، وعناوين العملاء) غالبا ما تجذب انتباه الجواسيسس المعلوماتيين اليها".[٥٤].

" ووفقا لرأى بعض الخبراء الأمنيين للحاسبات الالكترونية، فان سهولة اختراق انظمة تلك الحاسبات ، والوصول إلى ما تحوية من برامج وبيانات ومعلومات ، وترجع إلى عدة عوامل، أبرزها:

١- تسقط صناعة الحاسبات الآلية فى اندفاعها للانتاج والتسويق مسألة الامن من حسبانها لصالح رفع القدرة الوظيفية وتحسين مستوى الاداء فى الخدمة.

٢- توجه صناعة أجهزة الإتصال والحاسبات الآلية جل اهتمامها ، نحو

---

[٥٣]- شبه البعض الحاسبات الآلية بانها خزائن بلا ابواب، وفى ذلك يقول Kennth Weiss رئيس قسم الحاسبات الالية لدى شركة امريكية، انه " لو ادرك كبار المسئولين الادرايين حقيقة المسئولية والمخاطر المحملة التى تهدد اصول الشركات وسمعتها ، لاغلقوا جميع شبكات ومراكز الحاسبات الالية.

د/ هشام محمد فريد رستم، هامش (١) ص ١٣٢، د/ محمد سامى الشوا، هامش (٢)، ص ٢١٢..

[٥٤]- د/ هشام محمد فريد رستم، ص ١٣٢.

انتاج اسرع الوسائل للاتصال، دونما اهتمام موازن لحماية البرامج والمعلومات من الاعتراض غير المشروع والالتقاط، حتى لا تصطدم بارتفاع التكلفة وزيادة الاسعار.

٣- تزايد اعداد شبكات الحاسبات الآلية واتساع نطاقها بما قد يفوق القدرة على توفير الحماية لجميع اجزائها[٥٥].

مجالات التجسس المعلوماتى:

تتعدد مجالات التجسس المعلوماتى بتعدد مجالات واوجه النشاط المختلفة، فعلى سبيل المثال، نجد انه فى مجالات النشاط التجارى، ترتكز عمليات التجسس المعلوماتى، على كشف الأسرار التسويقية والتجارة (كحسابات التكلفة، وكشوف الميزانية، وحالة الأسواق، وعناوين العملاء.. وغيرها) وفى مجالات النشاط الصناعى والتقنى، تسعى عمليات التجسس - بصورة كبيرة- إلى (كشف نتائج الابحاث والتطوير ، والبيانات المتعلقة بعمليات الانتاج، وأسرار تصميمات المنتجات " لاسيما تصميمات الشرائح الصغيرة من أشباه المواصلات" ، وفى المجالات الامنية والعسكرية والاستخباراتية والنووية، تكثف نشاطات التجسس جهودها نحو اختراق النظم الامنية والعسكرية والاستخباراتية والنووية للوصول إلى ادق تفاصيل أسرار البيانات والمعلومات المتعلقة بتلك الشئون، بما يكون له من بالغ الاثر على امن وبقاء الدول والحكومات.

وللتجسس المعلوماتى أيضا فى مختلف المجالات ابعاد خطيرة غير مسبوقة، فالتكثيف المركز للمعلومات فى ذاكرات الحاسبات الآلية يجعلها هدفا مغريا لأى متلصص يملك خبرة كافية وتجهيزات جيدة، سيما مع امكانية الاستعانة بالحاسبات الآلية فى فرز المعلومات المخزنة وتصنيفها ونسخها بسهولة وسرعة فائقة، وبغير أن يتخلف عن ذلك اى اثر.

أساليب التجسس المعلوماتى:

" تتعد صور واشكال تخزين البيانات والمعلومات المعالجة الكترونيا ،فقد تكون تلك البيانات و المعلومات مخزنة على هيئة نبضات كهربائية فى دوائر الكترونية مجمعة، أو فى وسائط واوعية معينة" كالبطاقات الورقية المثقبة، والاشرطة والاقراص المغناطيسية" ، كما انها قد تكون فى حالة بث وانتقال من

[٥٥]- د/ محمد سامى الشوا، ص ٢١٢.

نهاية طرفية إلى اخرى، والتوصل غير المشروع إلى تلك البيانات والمعلومات له فى كل حالة من حالتى تخزين وانتقال البيانات والمعلومات السابقتين اساليبة.

١ـ أساليب التجسس والحصول على البيانات والمعلومات المخزنة:

وهذه الاساليب متعددة، ومتدرجة فى تعقيدها:

أـ فمن هذه الاساليب ماله طابع تقليدى، ومن قبيله: سرقة الاسطوانات التى تخزن فيها البيانات والمعلومات، ورشوة أو تهديد عاملين بالجهة المستهدفة. للكشف عن البيانات المخزنة داخل حاسباتها، والحاق موظفين بالجهة المستهدفة أيضا يتولون مهمة التجسس من خلال عملهم بها.

بـ- ومن هذه الاساليب ماله طابع فنى، وذلك مثل: دس وحدات ناقلة للبيانات داخل أجهزة الحاسب الآلى، وتوصيله كهربائيا بشكل خفى بكابل خارجى، ومعالجة الشرائط والاسطوانات الممغنطة التى لم تكمل الجهة المالكة لها محوها أو اتلافها لاعادة اظهار محتوياتها، واستظهار المعلومات التى تستخدم اوراق الكربون عند تدوينها بمعالجة اوراق الكربون المهملة، واخفاء برنامج "حصان طرواده"[٥٦]، فى البرامج التطبيقية بحيث يسمح بالوصول عن

[٥٦]- برنامج حصان طرواده Torjans هو برنامج خادع يخفى وراءه غرضا غير مشروع ، حيث يظهر كبرنامج عادى يؤدى بعض المهام المفيدة والمالوفة لمستخدمة ، بينما الحقيقة على النقيض من ذلك تماما، حيث يخفى هذا البرنامج داخله بعض الاوامر والتعليمات التى تؤدى عند تشغيله مهام ضارة غير متوقعة تمثل اغراضه الحقيقية المضمرة،وهكذا فقد يبدو البرنامج كما لو كان معدا لتنظيم البيانات بالملفات أو تكثيفها، بينما الهدف الحقيقى من وراء تشغيله قد يكون محو هذه البيانات، من ذاكرة الحاسب الآلى أو التهديد بذلك لابتزاز مستخدمة أو الاستيلاء على المال بتخريف البيانات المدخله أو المخزنة، وعادة ما توجد برامج احصنة طروادة فى برامج الاعمال (كبرامج معالجة النصوص، وبرنامج ادارة قواعد البيانات) وغالبا ما تكون مختفية فى منتصف البرنامج أو فى مكان غير مستعمل منه ، والبرنامج الذى يتضمها قد يعمل بطريقة صحيحة لعدة شهور قبل أن تظهر اعراض الاوامر غير المتوقعة وغير المشروعة، وقد تظهر هذه الاوامر وتنفذ مباشرة عند تشغيله ، وبرامج احصنة طرواده– وعلى خلاف ما يسمى بفيروسات الحاسبات الآلى- لا تنسخ نفسها ، واكتشافها بالغ الصعوبة، وكذلك ايضا محاولة اقتفاء اثر معدها، وقد تم نعت تلك البرامج بـ" برامج حصان طروادة" نظرا لخطورتها ، واثارها المدمرة، وقدرتها على الخداع، والمفاجاة والتضليل، مثلما فعل حصان طروادة الخشبى الكبير الذى ضم بداخله مجموعة من الجنود حينما احكم خداع جيش طروادة الذى كان يدافع عن ارضه حيال غزو اسبرطه لتلك المدينة، فعندما رآه اهل المدينة فرحوا به

بعد إلى قاعدة البيانات لقراءتها أو تعديلها بغير ان يشعر بذلك احد.

ج- كما يمكن أيضا باستخدام هوائيات متصلة بحاسب خاص التقاط وتسجيل ومعالجة الموجات الكهرومغناطيسية التى تنبعث من الحاسب الآلى اثناء تشغيلة ، وترجمتها إلى بيانات واضحة، وذلك من مسافة تبعد عن الحاسب المستهدف بما يزيد على الاف الكيلومترات.

د- كما يمكن كذلك استغلال ما يعرف " بالابواب الخفية أو الخليفة Back doors" والمعروفة أيضا باسم " ابواب المصيدة Trap doors" فى الوصول غير المشروع ،وغير المحدود إلى برامج وملفات بيانات النظام، اذ من المعتاد عند اعداد البرامج ترك ثغرات أو نقاط دخول غير معلن عنها تتجنب اجراءات الامن العادية، وذلك بهدف السماح باضافة تعليمات إلى البرامج لتلافى ما قد يظهر فيها من اخطاء ، ووجود هذه الثغرات قد لا يكون متعمدا دائما، حيث يمكن أن توجد عرضا فى بعض الاحيان نتيجة اخطاء فى التصميم الكلى للنظام أو نتيجة مواطن ضعف فى مجموعة الدارات الالكترونية للحاسبات الآلية ، وعندما يكون تركها مقصودا ، فانها تلغى فى الطبعة النهائية للبرنامج ، بيد أن هذا

وقاموا بادخاله داخل مدينة طروادة، وحينما استقر به الحال قام الغزاة بالخروج منه واستولوا على تلك المدينة، وفقا لما جاء بقصص الحرب التى راوها الشاعر الاغريقى القديم هوميروس فى ملحمتى الالياذة والأوديسة .

د/ هشام محمد فريد رستم- ص ٧٢- ٧٤، مهندس: احمد حسن خميس، المرجع السابق ، ص ٣٦.=

= ولمزيد من الايضاح ، فان برنامج حصان طراوده ما هو الا اسم لملف برنامج تجسس يتم ارساله وزرعة فى جهاز الضحية ليكون هو حلقة الوصل بين جهاز المخترق وجهاز الضحية، ويطلق على هذا البرنامج اسماء عديدة، منها الملف اللاصق أو الصامت أو ملف الباتش Patch files وهو الاسم الاشهر فى عالم الهاكرز، وهناك طرق عديدة لارسال هذا البرنامج وزراعته لعل أشهرها على الاطلاق هو استخدام البريد الالكترونى، حيث يقوم المخترق بارسال رسالة إلى الضحية ويرفق بها ملف حصان طرواده، ونظر لسذاجة الضحية أو عدم المامة بمضمون تلك الرسالة، فانه يقوم بفتحها وتحميل الملف المرفق بها اعتقادا منه أنه يمثل احد البرامج المفيدة، ثم يكتشف بعد ذلك أن هذا البرنامج لا يعمل فيظن أن به عطل ما فيهملة وكأن شيئا لم يكن، وفى ذلك الوقت يكون حصان طرواده قداخذ مكانه داخل نظام حاسب الضحية، وبدا فى مهامة التجسسية حتى وان قام الضحية بحذف البرنامج بعد ذلك فلا فائدة من ذلك فملف حصان طرواده يكفية أن يعمل لمرة واحدة فقط ليقوم بمهامة .

مهندس: احمد حسن خميس، المرجع نفسه ، ص ٣٦.

الالغاء قد يتم فى بعض الاحيان بصورة متعمدة اغفالة، وبذلك يكون متاحا- إذا ما وجدت عمداً أو عرضا ثغرات أو نقاط دخول – الوصول إلى اجزاء من النظام غير مصرح بولوجها، والاطلاع على ملف البيانات المخزنة داخله.

٢-أساليب التجسس والحصول على البيانات والمعلومات المتنقلة:

إذا كانت البيانات والمعلومات فى حالة انتقال فيما بين النهايات الطرفية، فان اساليب التجسس عليها والتقاطها تختلف باختلاف الوسيلة الناقلة.

أ- فالبيانات التى يجرى نقلها عبر الاسلاك المعدنية أو خطوط الهاتف المخصصة لنظم الإتصالات الالكترونية لا يحتاج معترضها لاكثر من مجرد جهاز التقاط بسيط يمكن تركيبه من وحدات الكترونية تتوافر فى الأسواق، وتثبيته بطريقة خفية داخل صناديق التوزيع التى تنتهى إليها معظم وسائل الإتصال السلكية واللاسلكية، وقد يضاف جهاز حث إلى جهاز الالتقاط كى يعمل فحسب حال وجود بيانات أو اشارات فى السلك أو الخط الذى تجرى مراقبته.

ب- أما المعترض لوصلات الموجة القصيرة المحتوية على حزمة من القنوات المحملة بالبيانات، فانه يستفيد مما ينتج عن بث هذه الموجات من نتوءات اشعاعية، جانبية وخلفية، فيستخدم فى مجال أحد هذه النتواءات أجهزة التقاط خاملة لا يصدر عنها أيه إشارات لاسلكية، مما يجعل من الصعب اكتشافها.

ج- وبالكيفية السابقة يمكن اعتراض الإتصالات التى تبث من المحطات الأرضية فى اتجاه الاقمار الصناعية، حيث يمكن أيضا استغلال ظاهرة النتواءات الجانبية والخلفية، أما الشعاع الذى يبثه القمر الصناعى إلى الأرض فإنه يغطى مساحة شاسعة منها تقدر بآلاف الأميال المربعة، ومن أى موقع فى نطاق هذه المساحة يمكن – باستخدام أجهزة خاصة- التقاط البيانات والمعلومات المرسلة ، حتى أن البيانات التى يجرى عن طريق قمر صناعى- على سبيل المثال – إرسالها من كاليفورنيا (جنوب الولايات المتحدة الأمريكية) إلى نيويورك (بشرقها) يمكن لمعترض فى فلوريدا (بالجنوب) إلتقاطها[٥٧].

[٥٧]- د/ هشام محمد فريد رستم- ص ١٤٠- ١٤٣.

المطلب السادس

الإتلاف المعلوماتى

يقصد بالاتلاف المعلوماتى أو التخريب المنطقى أو تدمير نظم المعلومات " مدى صلاحية البرامج و المعلومات المعالجة آليا لآن تكون محلا يرد عليه العدوان فى جريمة الإتلاف، عندما لا يترتب على المساس بها أى إتلاف لأى من العناصر المادية التى يتكون نظام المعالجة الآلية للمعلومات".

وتتعدد الاساليب والوسائل التى يستخدمها الجناة فى جرائم المعلوماتية لإتلاف برامج الحاسب الآلى، والبيانات والمعلومات المعالجة والمخزنة آليا، والتلاعب بها ، وتختلف تلك الأساليب أيضا باختلاف اغراض الجناة من حالة لأخرى.

والاتلاف المعلوماتى إما أن يكون عن عمد وقصد، وإما أن يكون بغير قصد ، كما أن هذا الاتلاف قد يكون كليا يتمثل فى محو البرامج والمعلومات المخزنة داخل جهاز الحاسب الآلى كلياً،وقد يكون جزئياً، ويطلق عليه فى هذه الحالة (تشويه أو تعبيب) ويتمثل فى ادخال فيروس داخل الجهاز بحيث يعمل على التقليل من كفاءته أو يبطئ حركة الجهاز ذاته[٥٨].

أساليب التخريب المنطقى للبرامج والمعلومات:

ينصب الاتلاف المعلوماتى أو التخريب المنطقى للحاسب الآلى ومكونات على الكيانات المنطقية له، والتى تتمثل – كما سبق أن ذكرنا- فى مجموعة من الاوامر والتعليمات اللازمة لتشغيل اجهزة الحاسب الآلى وإنجاز مهامة واكثر ما يتم التوسل به لتنفيذ التخريب المنطقى هو البرامج ذات الأثر التدميرى التى تستهدف محو جزء أو كل برامج أو ملفات الحاسب أو البيانات و المعلومات المخزنة به، وكذلك أيضا سائر البرامج الخبيثة التى تصيب نظام الحاسب الالكترونى بالشلل والعطب، وهذه البرامج متعددة ، ولكل برنامج منها تسمية شائعة تعبر عن وظائفة التخريبية والضرر الذى يمكن أن يلحقة بهذا الحاسب ومكوناته [٥٩]، ولعل أبرز ما اثار منها مشكلات فنية، وتسبب فى خسائر مادية فادحة ما يلى:

---

[٥٨]- انظر: محمد أمين الرومى- جرائم الكمبيوتر والأنترنت –دار المطبوعات الجامعية الاسكندرية ٢٠٠٣ - صفحة ٥٦.

[٥٩]- د. هشام محمد فريد رستم، ص ١٥٨.

أولا: استخدام برامج القنابل المنطقية Logic Bomby:

القنبلة المنطقية عبارة عن برنامج أو جزء من برنامج ينفذ فى لحظة محددة أو كل فترة زمنية منتظمة، ويتم وضعه فى شبكة معلوماتية بهدف تحديد ظروف أو حالة مضمون النظام بغية تسهيل تنفيذ عمل أو غرض غير مشروع(٦٠).

وعلى سبيل المثال، فإنه يمكن إدراج تعليمات فى برنامج نظام التشغيل وينصب البحث بعد ذلك على عمل معين يمكن أن يكون محلاً للاعتداء، كأن تسعى قنبلة منطقية إلى البحث عن حرف معين وليكن (أ) فى اى سجل يتضمن أمراً بالدفع، وعندما تكتشفة، تحرك متتالية منطقية تعمل على إزالة هذا الحرف من السجل(٦١).

أمثلة للتخريب المنطقى بواسطة استخدام برامج القنبلة المنطقية:

١- فى الدانمارك، تمكن خبير فى نظم المعلومات من وضع قنبلة منطقية فى نظام احدى الحاسبات، ترتب عليه محو أكثر من مائة برنامج، وقد تم أيضا محو النسخ الاحتياطية لهذه البرامج عند تشغيلها نتيجة انتقال اثار القنبلة إليها، وتم ضبط الجانى، وقد عاقبة القضاء الدانمركى بالحبس لمدة سبعة اشهر (٦٢).

٢- قام مبرمج نظم سابق بإحدى الشركات الكبرى فى فورت ورث بولاية تكساس الامريكية عام ١٩٨٥ بالدخول إلى نظام معلومات حاسب تلك الشركة، بعد عدة أيام من الاستغناء عنه، معتمداً على معرفته لكلمة السر التى لم تقم الشركة بتغييرها، ووضع فية قنبلة منطقية من شأنها محو كل سجلات عمولة المبيعات مرة كل شهر، ولم يتم اكتشاف هذه القنبلة ووقف مفعولها إلا بعد أن محت أكثر من ١٦٨ ألف سجل من سجلات عمولة المبيعات الخاصة بتلك الشركة (٦٣).

٣- ومن الحالات فائقة الخطر للقنابل المنطقية التى يذكرها بعض الخبراء

٦٠- أنظر : د/ محمد سامى الشوا، ص ١٩٤، أ. محمد أمين الرومى، ص ٥٦.

٦١-أنظر : د/ محمد سامى الشوا، ص ١٩٥.

٦٢- أنظر : د/ محمد سامى الشوا، ص ١٩٦، د. هشام رستم ، ص١٦٠.

٦٣-أنظر : د/ هشام محمد فريد رستم ، ص١٦٠.

والمتخصصين فى مجال علوم الحاسبات الآلية، إخفاء قنابل منطقية، وبرامج أحصنة طرواده كذلك، فى البرامج المعلوماتية التى تبيعها دولة لأخرى، مثلما كانت بعض الدول تقوم بإخفاء قنابل منطقية فى البرامج التى كانت تبيعها للاتحاد السوفيتى (قبل تفككه)[٦٤].

ثانيا: استخدام برنامج القنبلة الزمنية أو الموقوتة Time Bombs

القنبلة الزمنية أو الموقوتة على عكس القنبلة المنطقية تماما، هى برامج مصممة بحيث تبقى ساكنة وغير فعالة ، وغير مكتشفة بالتالى لمدد قد تصل إلى اشهر ، بل وحتى أعوام، وهذه المدة يحددها عادة مؤشر زمنى يحتوية البرنامج – كتاريخ معين- بحيث ينشط برنامج القنبلة عند حلولة، ويؤدى مهامة التدميرية الهدامة[٦٥] ، وتثير القنبلة الزمنية- على النحو السابق بيانه- حدثا فى لحظة زمنية محددة بالساعة أو اليوم أو السنة، ومن ثم تنطلق أو تنفجر فى زمن وتاريخ محدد من السنة، فهى مرتبطة دائما بعنصر الزمن، فيتم إدخالها فى برنامج، وتنفذ فى جزء من المللى ثانية أو فى بضع ثوان أو دقائق وفقا للتحديد أو البرمجة اللازمة للانفجار، فعلى سبيل المثال يمكن ضبط القنبلة الزمنية أو الموقوته لكى تنفجر بعد شهرين فى يوم محدد وساعة محددة، لتحول مبلغا من النقود من حساب شخص معين فى اللحظة التى يكون فيها مرتكب الجريمة متواجدا فى بلدة اخرى غير بلدة المجنى عليه[٦٦].

أمثلة لتدمير نظم المعلومات عن طريق استخدام برنامج القنبلة الزمنية:

١- فى فرنسا، قام محاسب من الخبراء فى نظم المعلومات – وبدافع الانتقام على أثر فصلة من المنشأة التى يعمل بها- بوضع قنبلة زمنية فى شبكة المعلومات الخاصة بتلك المنشأة، بحيث تنفجر تلك القنبلة بعد مضى ستة اشهر من رحيلة عن المنشأة، وترتب على ذلك أن حدث إتلاف لكل البيانات الخاصة بها [٦٧].

---

[٦٤]-أنظر : د/ هشام محمد فريد رستم ، ص١٦٠.

[٦٥]-أنظر : د/ هشام محمد فريد رستم ، ص١٥٨.

[٦٦]-أنظر : د/ محمد سامى الشوا، ص ١٩٥.

[٦٧]-أنظر : د/ هشام رستم ، ص ١٥٩، د. محمد سامى الشوا، ص ١٩٦، أ. محمد أمين الرومى، ص ٥٧.

٢- فى المانيا الديمقراطية (سابقا) ، قام مبرمج بزرع البرنامج الذى يحول القنبلة الزمنية فى النظام المعلوماتى الخاص بالشركة التى يعمل بها، وتم برمجة القنبلة- بالتالى- بحيث يتعين أن تنفجر بعد عامين من فصله من الشركة، وفى حوالى الساعة الثالثة مساءا، وكما سجل هذا الجانى فى البرنامج الخاص بتلك القنبلة ، فان الاستفهام الخاص بيوم وساعة وسنة التنفيذ ظل مستمراً وكان هذا الشخص متأكداً من أن لحظة التدمير ستراعى بكل دقة، وبسبب ظرف طارئ أدى إلى أنهيار النظام- "لحظة تفجير القنبلة الموقوتة" – فإن أكثر من ٣٠٠ طرفية ظلت لا تعمل لبضعة ايام، وكان من الصعب اكتشاف الفاعل نظرا للتفاوت فى الزمن بين لحظة ارتكاب الفعل ولحظة النتيجة الاجرامية[٦٨].

[٦٨]-أنظر : د/ محمد سامى الشوا، ص ١٩٥- ١٩٦، أ. محمد أمين الرومى، ص ٥٧.

ثالثا: استخدام برامج الدودة Worm Software:

تعرف برامج الدودة بأنها " تلك البرامج التى تستغل ايه فجوات فى نظم تشغيل الحاسب الآلى، لتنتقل من حاسب الى آخر مغطية شبكة باكملها، لتحدث فى النهاية آثارها التخريبية"، وقد تنتقل تلك البرامج من شبكة إلى اخرى عبر الوصلات Links التى ترتبط بينها، واثناء عملية انتقالها تتكاثر – كالبكتريا- بانتاج نسخ منها، ومن اهم اهداف تلك البرامج شغل اكبر مجال ممكن من سعة الشبكة، وبالتالى تقليل أو خفض كفاءتها، وقد تتعدى اهدافها ذلك لتبدأ بعد التكاثر والانتشار فى التخريب الفعلى للملفات والبرامج ونظم التشغيل وبروتوكولات الإتصال [٦٩].

امثلة للإتلاف المعلوماتى عن طريق اسخدام برامج الدودة:

١- من أمثلة برامج الدودة التى ذاع صيتها بعد استخدامها ، برنامج اعده طالب بجامعة Clausthal- Zellerfeld بالمانيا الغربية (سابقا) لارسال تهئنة وتحية من خلال الحاسبات بمناسبة عيد الميلاد فى ديسمبر ١٩٨٧، وقد صمم هذا البرنامج بحيث يقرأ عناوين البريد الالكترونى المخزنة فى ذاكرة كل حاسب يصل اليه، ويرسل بعد ذلك تهئنة إلى اصحاب تلك العناوين، ثم ينتج نسخة من نفسه ويرسلها إلى كل الحاسبات المتصلة بالحاسب المضيف.. وهكذا دواليك، وكانت النتيجة أن استمر هذا البرنامج – بعد دخوله شبكة VNET التابعة لشركة IBM والتى تربط بين حاسبات فى ٤٥ دولة- فى التكاثر التسلسلى، إلى أن غطى فى غضون ساعتين اكثر من نصف مليون حاسب، مما ادى إلى انهيار قدرة الشبكة على تحمل تدفق الخدمات المرسلة، وتعطلها لمدة يومين تقريبا تم خلالها استئصال البرنامج من النظام [٧٠].

٢- من امثلة برامج الدودة أيضا ما يعرف بـ "Internet Worm" والذى عن طريقة تمكن طالب امريكى يدعى" روبرت موريس" – وكان طالب دراسات عليا فى جامعة كورنيل بولاية نيويورك- من تدمير ١٦ الف شبكة حاسب آلى منتشرة فى ارجاء الولايات المتحدة الامريكية ، وترتب على ذلك الهجوم أن حدثت خسائر فادحة، تمثلت فى تأخير الابحاث لآلاف الساعات، وفى اعادة البرمجة بتكاليف

---

[٦٩]-أنظر : د/ هشام محمد فريد رستم ، ص ١٦١.

[٧٠]-أنظر : د/ هشام محمد فريد رستم ، ص ١٦١

بلغت عدة ملايين من الدولارات [٧١].

٣- تم اكتشاف حالة من برامج الدودة اطلق عليها مصطلح " البرامج الدودية ضد القتلة مستخدمى الذرة" ويرمز اليها برمز "WANK" حيث غزت تلك البرامج مرتين خلال عام١٩٨٩ شبكة علوم الارض والفضاء بالولايات المتحدة الامريكية، كنوع من أنواع الاحتجاج على اطلاق مكوك فضاء يحمل مجسما فضائياً مغطى ببودرة نووية[٧٢]

رابعا: استخدام فيروسات الحاسب الآلى Programms virus

التعريف بفيروسات الحاسب الآلى

تعددت تعريفات الفيروسات التى تصيب الحاسبات الآلية ومكوناتها المنطقية وتؤدى إلى اتلافها وتدميرها لدى المتخصصين فى جرائم المعلوماتية[٧٣]، فمنهم من عرفها بانها" مجموعة من التعليمات المرمزة"

---

[٧١]- اطلق البعض على هذا البرنامج اسم "Inter net" (نسبة إلى الشبكة التى اصابها بالعطب) واسماء اخرون " دودة موريس Morist Worm" (نسبة إلى معد روبرت ت. موريس الذى كان يبلغ من العمر ٢٣ عاما) وقد ادخل هذا البرنامج إلى شبكة انترنت مساء يوم ٣ نوفمبر ١٩٨٨، من خلال احدى وسائل التدقيق adebug feature فى حزمة البرامج الخاصة بالبريد الالكترونى، حيث بحث دخوله عن طريق =" باب خفى" من خلال كلمة سر بسيطة ليصل النظم الاخرى المرتبطة بالشبكة، وفى مدة لا تتجاوز الاربع والعشرين ساعة كان هذا البرنامج قد انتشر عبر تلك الشبكة وغطى اطرافها كليا، وقد تاثرت به ثلاث شبكات كبرى مرتبطة، شبكة انترنت، وهى (شبكات اربانت ARPA NET ، وشبكة هيئة مشروعات الابحاث المتقدمة الولايات المتحدة الامريكية وتعرف باحرفها الاولى، وترتبط تلك الشبكة حاسبات مدنية، باخرى عسكرية، وميلنت MIL Net وهى الشبكة العسكرية Military Network، وهى تتبع وزارة الدفاع الامريكية، وتستخدم فى الاتصالات العسكرية التى لا تتسم بدرجة عالية من السرية ،وتعرف وفقا لاحرفها الاولى" وشبكة أن. أس إف نت NSF Net وهى شبكة مؤسسة العلوم القومية الامريكية وترتبط بين الجامعات ومعاهد الابحاث ومصادر علمية كثيرة، وتعرف ايضا بأحرنها الأولى ، كما تاثر به اكثر من ستة الاف حاسب آلى فى ارجاء الولايات المتحدة الامريكية المختلفة، قام هذا البرنامج بملء ذاكراتها حتى لم يعد بمقدورها القيام باى عمل.

د. هشام محمد فريد رستم ، ص ١٦٣، د. محمد سامى الشوا، ص ١٩٤، أ. محمد أمين الرومى، ص ٥٨.

[٧٢]- د. محمد سامى الشوا، ص ١٩٤، أ. محمد أمين الرومى، ص ٥٨.

[٧٣]- يرجع الفضل فى وضع اول تصور لفيروس معلوماتى إلى الدكتور "فريد كوهن" فى الحلقة

(المكودة) ، تنتج لنفسها نسخا مطابقة تلحق من تلقاء ذاتها ببرامج التطبيقات ومكونات النظام المنفذ لتقوم فى مرحلة معينة بالتحكم فى اداء النظام الذى اصابته[٧٤]، ومنهم من عرفها بانها " مجموعة من التعليمات التى تتكاثر بمعدل سريع جدا لدرجة تصيب النظام المعلوماتى بالشلل التام" أو هى" خلايا كهرومغناطيسية نائمة ومبرمجة بحيث تنشط فى وقت محدد لتخريب البرنامج الاصلى، وتنتشر فى الاجهزة الاخرى التى تضمها الشبكة بحيث تفسد ما تحتوية من معلومات" [٧٥]، ومنهم من عرف الفيروس أيضا بانه" برنامج حاسب مثل اى برنامج تطبيقى آخر، ولكن يتم تصميمة بواسطة احد المخربين بهدف محدد، وهو احداث اكبر ضرر ممكن بنظام الحاسب ، ولتنفيذ ذلك يتم اعطاؤه القدرة على ربط نفسه بالبرامج الاخرى، وكذلك اعادة انشاء نفسه حتى يبدو وكانه يتكاثر ويتوالد ذاتيا، وهذا ما يتيح له قدرة كبيرة على الانتشار ببرامج الحاسب المختلفة ، وكذلك بين مواقع مختلفة فى الذاكرة حتى يحقق اهدافه التدميرية"[٧٦] ، كما عرفه المركز القومى للحاسب الآلى بالولايات المتحدة الامريكية فى تقرير أعده حول الإعتبارات الامنية فى الحاسبات الشخصية بانه " برامج مهاجمة تصيب انظمة الحاسبات باسلوب يماثل إلى حد كبير اسلوب الفيروسات الحيوية التى تصيب الانسان، وهو فى العادة برنامج صغير مكتوب بلغة متدنية المستوى مثل "لغة التجميع" مما يزيد من صعوبة اكتشافه، ويقوم بالتجول فى الحاسب الآلى باحثا عن برنامج غير مصاب، وعندما يجد واحداً ينتج نسخة من نفسه لتدخل فيه، وتتم عملية الادخال هذه فى جزء من الثانية، حيث يقوم البرنامج المصاب فيما بعد بتنفيذ اوامر الفيروس[٧٧].

الدراسية الاسبوعية التى القاها بجامعة جنوب كاليفورنيا بالولايات المتحدة الامريكية عن امنية الحاسب الآلى – وذلك فى نوفمبر ١٩٨٣، حيث قام دكتور كوهن بتعريف الفيروس على أنه "برنامج يصيب البرامج الاخرى حيث يعدل فيها عن طريق ادخال نسخة منه فيها يقوم بانتاجها ، ولديه القدرة على تطوير نفسه خلال عملية اعادة انتاج نفسه، ويمكنه الانتشار فى النظام أو الشبكة ليسبب فى البرنامج والبيانات تغيرات تحكمية".

د. هشام محمد فريد رستم ، ص ١٦٤، هامش (١).

[٧٤]- أنظر : د/ هشام محمد فريد رستم ، ص ١٦٣.

[٧٥]-أنظر : د/ محمد سامى الشوا، ص ١٨٩.

[٧٦]- أنظر : أ/ محمد أمين الرومى، ص ٢٦.

[٧٧]- الفيروس – سواء كان حيويا ام الكترونيا- يمثل بشكل اساسى- كما يقول " فيليب المر دى وت" –

خللا فى المعلومات، فالفيروس الحيوى عبارة عن نبذ صغير جدا من الشفرة الوراثية التى تستطيع ان تسيطر على آليه الخلية الحية وان تخدعها بحيث تقوم تلك الخلية نفسها بصنع آلاف النسخ المماثلة من الفيروس الأصلى، وعلى نفس النحو، يحمل فيروس الحاسب ضمن تعليماته الوصفة اللازمة لصنع نماذج مطابقة له، وعندما يصاب حاسب ما بفيروس نمطى، فان هذا الاخير يسيطر على نظام تشغيل القرص، وبعدئذ، ومع كل اتصال للحاسب المصاب مع جزء غير مصاب من البرنامج، فان نسخة جديدة من الفيروس تنتقل إلى هذا البرنامج الجديد، وبهذا الشكل تنتشر العدوى من حاسب إلى اخر بواسطة مستخدمى الحاسبات أنفسهم الذين يتبادلون الاقراص فيما بينهم، أو الذين يرسلون البرامج إلى بعضهم البعض عبر خطوط التليفون من خلال الشبكة العالمية للإتصالات والمعلومات (انترنت) .

د. هشام محمد فريد رستم ، هامش (١) ص ١٦٤.

خصائص فيروسات الحاسب الآلى

تتمتع فيروسات الحاسب الآلى بقدرة عالية جدا على مهاجمة اجهزة الحاسبات الآلية والشبكة العامة والخاصة، وتسفر تلك المهاجمة عن تدمير للبرامج والبيانات والمعلومات المخزنة آليا، وتعويق للاتصالات، وتشوية للبيانات والمعلومات، بل وفى احيان كثيرة فانها تضلل المستخدم ببيانات خاطئة، وتتسلل تلك الفيروسات إلى الحاسبات الآلية التى ضمت عند اتصالها باحدى الشبكات الملوثة بها، أو عند نقل برنامج مصاب لذاكرة الحاسب الآلى، حيث لا تلبث أن تتكاثر خفية ودون دراية من المستخدم أو من نظام تشغيل الحاسب، وتقوم بعملها بسرعة وحذر فى أول الأمر، وما تلبث أن تتمكن من حاسب الضحية حتى تحدث آثارها التدميرية وتصيبة بالشلل التام[٧٨].

ولعل أهم ما يميز فيروسات الحاسب الآلى عن غيرها من البرامج التخريبية الاخرى هو انتاجها نسخا من نفسها، وقدرتها اثناء عملية الانتاج الذاتى على التغير والتطور والتكيف مع البرامج المتنوعة (وإن كان بامكانها أن تحدث طفرة) وتمتعها إلى حد ما بقدر من الذاتية، وامكانية تسببها فى احداث كافة انواع الآثار الضارة لنظام الحاسب الآلى " بدءا من مجرد عرض عبارات أو رسوم على الشاشة، مروراً بتغيير البيانات والمعلومات أو محوها، وانتهاءا بتدمير النظام باكمله" والخطر الاساسى للفيروس المعلوماتى يكمن فى امكانية استجماعه سائر مقومات التخريب الموزعة على ما عداه من برامج مخربة، اضف إلى ذلك سرعة انتشاره، وتغير شكل ومضمون النسخ التى ينتجها من نفسه حتى تتكيف مع المحيط الذى تستقر فيه، وامكانية استخدامه فى احداث تغيير لوغارتمى للبيانات أو محوها أو تدمير نظام الحاسب باكمله كما سبق منذ قليل[٧٩].

وعموما ، فانه يمكن اجمال خصائص فيروسات الحاسب الآلى فيما يلى:

١- القدرة الفائقة على الاختفاء : فالفيروس ما هو الا برنامج له القدرة على اخفاء نفسة عن الضحية مستخدم جهاز الحاسب الآلى ، ويستخدم فى اخفاء نفسه وسائل متعددة، منها – على سبيل المثال- ارتباطه بالبرامج شائعة الاستخدام، حيث أن كل مستخدم للحاسب الآلى يهتم بتوفير اكبر قدر ممكن من

---

[٧٨]- أنظر : د / محمد سامى الشوا، ص ١٨٩- ص ١٩٠.

[٧٩]- أنظر : د / هشام محمد فريد رستم ، ص ١٦٥.

البرامج التى تمكنه من الاستفادة بخصائص حاسبة الشخصى، واغلب المستخدمين يقومون بنسخ هذه البرامج دون السؤال عن مصدرها أو كنهها، وعند تشغيلها ينتقل الفيروس إلى القرص الصلب ويقوم باداء اعماله التخريبية، بل أن هناك من الفيروسات ما يدخل إلى الحاسب الآلى كملفات متخفية، بحيث لا يستطيع المستخدم فى اغلب الاحيان ملاحظة وجودها على شاشات الحاسبات الآلية عن طريق فهرس الملفات، وبعض الفيروسات تقوم بالاستقرار فى اماكن معينة يصعب على المستخدم ملاحظتها " مثل الذاكرة" وتنتظر فى هذا المكان حتى تشير الساعة إلى تاريخ معين فتقوم بتشغيل نفسها وتنفيذ اعمالها التدميرية، كما أن بعض الفيروسات تقوم باخفاء اى اثر يدل على وجودها، حيث تظل البرامج المحتوية عليها تعمل بكفاءة دون اخطاء ولمدد طويلة، وفى ذات الوقت يقوم الفيروس بالانتقال من برنامج إلى اخر بخفة وروية.

٢- الانتشار: لفيروس الحاسب الآلى قدرة فائقة على الانتشار- كما سبق القول- تفوق قدرة الفيروس الحيوى أو البيولوجى، فعلى سبيل المثال، فانه يمكن لفيروس حاسب آلى أن ينتقل إلى الملايين من اجهزة الحاسبات الآلية الخاصة بالمتسخدمين الضحايا فى نفس الوقت، كمايمكن فى ثوان معدودة أن ينتقل من قارة إلى اخرى.

٣- القدرة على الاختراق: تتمتع فيروسات الحاسبات الآلية أيضا بقدرة فائقة على اختراق نظام البيانات والمعلومات بالحاسب الآلى وكذلك الموانع التى يقيمها المستخدم.

٤- القدرة على التدمير: عندما يدخل فيروس الحاسب الآلى إلى جهاز الحاسب الخاص بالضحية، فانه يظل ساكنا حتى تبدأ لحظة الصفر التى يبدأ عندها فى النشاط والحركة، وساعة الصفر هذه اما أن تكون كلمة معينة يكتبها مستخدم الحاسب الآلى أو الجانى المعلوماتى ، أو اشارة معينة أو عند تاريخ معين فى السنة، ويعمل الفيروس غالبا على مسح البيانات والمعلومات المخزنة فى ذاكرة الحاسب الآلى أو على تدمير نظام الحاسب باكمله [٨٠].

الاضرار الناشئة عن استخدام فيروسات الحاسب الآلى:

لفيروسات الحاسبات الآلية اثار وخيمة يصعب حصرها والاحاطة بها وإدراكها، وسوف نورد فيما يلى بعض الاضرار التى تصيب الحاسبات الآلية

[٨٠]- أنظر : أ/ محمد أمين الرومى، ص ٢٨-٢٩ .

ومكوناتها المنطقية نتيجة استهدافها عن طريق الفيروسات المعلوماتية:

١- فقد الملفات المعلوماتية من الذاكرة : حيث يقوم الفيروس المعلوماتى بمسح اجزاء من الملفات المخزنة" فى حالة الاتلاف الجزئى للبرامج والبيانات المخزنة آليا" أو يقوم بمسح الملفات المخزنة فى الحاسب الآلى بأكملها " وذلك فى حالة الاتلاف الكلى لذاكرة الحاسب الآلى ونظامه.

٢- ملء ذاكرة الحاسب الآلى بالنفايات.

٣- كتابة رسالة على الشاشة وذلك فى غالبية الفيروسات الحميدة.

٤- ابطاء تشغيل الجهاز، بحيث يستغرق وقتا أطول من المعتاد لتجميع البيانات ومعالجتها.

٥- تغيير وظائف المفاتيح من على لوحة المفاتيح، مما يؤدى إلى صعوبة استخدام الجهاز .

٦- إتلاف البرامج والمعلومات اوتدميرها جزئيا.

٧- نسخ البرامج و المعلومات من مستخدم إلى مستخدم مما يشكل خطورة بالغة، حيث أن هذه البرامج و المعلومات غالبا ما تحتوى على اسرار ومعلومات ذات قيمة مالية كبيرة"[٨١].

انواع فيروسات الحاسب الآلى:

تتعدد انواع الفيروسات المعلوماتية التى تستخدم فى التخريب المنطقى لبرامج وبيانات الحاسب المخزنة اليا، ويقسم الفقة تلك الفيروسات من حيث تكونيها واهدافها إلى ما يلى:

أ- فيروس عام العدوى: وهو ذلك الفيروس الذى ينتقل إلى اى برنامج و ملف معلوماتى.

ب- فيروس محدد العدوى: وهو ذلك الفيروس الذى يستهدف نوعا محددا من النظم لينتقل إليه ويهاجمه، ويتميز هذا النوع عن النوع السابق بانه أبطأ فى الانتشار واصعب فى الاكتشاف.

ج- فيروس عام الهدف : وتندرج تحت هذا النوع من الفيروسات الغالبية العظمى التى تم اكتشافها حتى الآن، ويرجع ذلك إلى سهولة اعداد تلك الفيروسات،

[٨١]-أنظر : أ/ محمد أمين الرومى، ص ٢٩- ٣٠.

واتساع مدى تخريبها.

د- فيروس محدد الهدف : ويحتاج إعداده إلى درجة غالية من الكفاءة والمهارة، والى دراية تامة بالتطبيق أو الهدف أو الغرض الذى يستهدفه، وقد يجرى هذا الفيروس تلاعبا ماليا أو يدخل تعديلات فى تطبيق عسكرى، وبعضه قد ينهى وجوده بعد تنفيذ هدفه،وتكمن خطورة بعض الفيروسات من هذا النوع فى انها لا تؤدى إلى تعطيل عمل البرنامج، بل تبدل فحسب من هدفها"[٨٢].

[٨٢]-أنظر : د/ هشام محمد فريد رستم ، ص ١٦٦، د. محمد سامى الشوا، ص ١٩١.

المبحث الثانى
الجرائم التى ترتكب بواسطة الحاسب الألى ومكوناته

نتناول هذا المبحث من خلال تسعة مطالب على النحو التالى:
المطلب الأول: الاحتيال المعلوماتى
المطلب الثانى: التزوير المعلوماتى
المطلب الثالث: النصب المعلوماتى
المطلب الرابع : جرائم الاعتداء على حرية الحياة الخاصة
المطلب الخامس: جرائم الاعتداء على حقوق الملكية الفكرية والادبية.
المطلب السادس: جرائم إفشاء الاسرار فى اطار المعلوماتية
المطلب السابع: جرائم السب والقذف عبر الإنترنت.
المطلب الثامن: الجرائم المخلة بالآداب العامة فى اطار المعلوماتية
المطلب التاسع : غسيل الأموال عبر الإنترنت

المطلب الأول
الاحتيال المعلوماتى

ينصرف اصطلاح الاحتيال بوجه عام إلى الغش والخداع الذى يعمد إليه أى شخص للحصول من الغير بدون وجه حق على فائدة أو منفعة أو ميزة ما، ويقصد بالاحتيال المعلوماتى إساءة استخدام الحاسبات الآلية والتلاعب فى نظم المعالجة الإلكترونية للبيانات والمعلومات للحصول بغير حق على اموال أو اصول أو خدمات.

ويتميز الاحتيال المعلوماتى عن غيره من انماط الاحتيال التقليدى أو العادى بالتعقيد الناجم عن استخدام المفاتيح والشفرات والدلائل الإلكترونية فى ارتكابة، ونظره الكثيرين إليه باعتباره نوعا من التحدى الذهنى الذى يثير الرغبة فى اتيانة، وامكانية اقترافه عن بعد، وعدم تركه آثار مادية تدل على وقوعه بالاضافة إلى فداحة خسائرة وسهولة طمسة واخفائه.

ولعل الهدف الرئيسى للتلاعب الذى يتحقق به الاحتيال المعلوماتى فى

قطاع المعلومات هو البيانات التى تمثل فى نظم معلومات الحاسبات الإلكترونية اموالا أو أصولاً وموجودات، واكثر البيانات استهدافا لهذا التلاعب هوالمتعلق منها بالمستحقات المالية والايداعات المصرفية وتقديرات الائتمان وحسابات ونتائج الميزانيات، واكثر ما يرد عليه هذا التلاعب – وفقا لماتم الكشف عنه من حالات الاحتيال والغش المعلوماتى– هو حسابات المرتبات والمعاشات واوامر الدفع وحسابات التكلفة والنفقات ، بالاضافة إلى قوائم المبيعات وكشوف الاعانات الاجتماعية ، والحسابات المعدة بواسطة الحاسبات الآلية لميزانيات البنوك والشركات وقطاعات الاعمال.. وغيرها، اما اكثر صور الاحتيال المعلوماتى اضرارا وخطرا على الانشطة الاقتصادية والاقتصاد القومى ككل ، فتتمثل فيما يقع منه على انظمة التحويل الالكترونى للاموال والودائع المصرفية أو ما يسمى " بالأموال الإلكترونية أو الافتراضية" نظرا لضخامة حجم ما يتم تداوله عبر هذه الانظمة من اموال، واختزالها- اى تلك الانظمة- كذلك المسافات بما يتيح تنفيذ الاحتيال عبر الحدود الاقليمية للعديد من الدول، واختزالها أيضا الزمن اللازم لاتمام التعاملات والتحولات المالية، وكذا الزمن اللازم لسلب الاموال بالاحتيال والغش إلى ثوان معدودة، وهو ما انعكس من جهة فى صيروره الأموال المتداولة عبر هذه الانظمة هدفاً من اهداف الجريمة المنظمة والقوى الخارجية المعادية، وفى فداحة الخسائر الناجمة عن عمليات الاحتيال الواقعة فى محيط هذه الانظمة من جهة اخرى.

ومن المتوقع تفاقم خطر هذه الصور من الاحتيال المعلوماتى فى المستقبل اكثر مما هى عليه الآن، نظرا لاطراد الاعتماد على الانظمة الإلكترونية فى تحويل ونقل الاعتمادات والأموال والودائع، وتسارع وتيرة تحول المجتمع إلى مجتمع لا يتداول النقود ولا الشيكات[٨٣].

وتتعدد الاساليب التى ترتكب بهاافعال الإحتيال والغش المعلوماتى، ويجمعها كلها رباط يتمثل فى التعدى على البرامج والمعلومات المخزنة آليا، والتلاعب فيها للحصول بغير حق على اموال أو اصول أو خدمات، وتحقيق العديد من الاغراض الاجرامية الاخرى، وتفصيل ذلك فيما يلى:

التعدى على المعلومات والبرامج بغية تحقيق اغراضا غير مشروعة:

تتحقق تلك الجرائم بواسطة العديد من الافعال الاجرامية، التى تمثل

[٨٣]- أنظر : د/ هشام محمد فريد رستم ، ص ٤٥- ٤٩.

السمة العالية لافعال تعدى المحتالين والتى تتجسد فى صورة المعالجة غير المشروعة- سواء للمعلومات والبيانات المخزنة آليا أو للبرامج ذاتها – بغرض تحقيق العديد من الاهداف الاجرامية غير المشروعة.

اولا: التعدى على المعلومات والبيانات المخزنة آليا:

يعد التلاعب فى المعلومات والبيانات المعالجة إلكترونيا – وفقا لاراء الخبراء والمتخصصين فى مجال الحاسبات الآلية- من اكثر افعال الغش ارتكاباً فى دول العالم المختلفة، وعلى وجه الخصوص فى اوروبا والولايات المتحدة الامريكية، ويتم ذلك التلاعب اما عن طريق ادخال معلومات مصطنعة أو اتلاف المعلومات الموجودة بالفعل فى الحاسب الآلى.

١- ادخال معلومات مصطنعة:

وترتكب تلك الجرائم المعلوماتية فى اغلب صورها عن طريق المسئول عن القسم المعلوماتى، والذى يسند إليه على وجه الخصوص وظيفة المحاسبة والمعاملات المالية، حيث يعتبر فى افضل وضع يؤهله لارتكاب هذا النمط من التلاعب غير المشروع، ويبدو أن الغش فى الدفع هو الاكثر تكراراً والاكثر سهولة أيضا فى تنفيذ تلك الجرائم، لاسيما فى وسط منشاة تملك قدراً كبيراً من النقود، وتتحقق تلك الصورة من جرائم المعلوماتية عن طريق عدة اشكال تجلت فى الواقع العملى الملموس، نذكر منها:

أ- ضم مستخدمين غير موجودين فى الواقع:

وينطبق ذلك على وجه الخصوص بالنسبة لمنشاة نضم العديد من الفروع، والتى يتغير عدد مستخدميها وفقا للظروف الاقتصادية وقائمة الطلبات، حيث يقدم مدير احد هذه الفروع معلومات وهمية إلى الادارة المركزية تتعلق باستئجار مستخدمين مؤقتين، ويكفى بالنسبة له- وفى نهاية كل تعد – أن يستلم الشيكات النقدية الخاصة بالمستخدمين المؤقتين: المزعومين، وقد وقعت شركة ASSE- DIC على سبيل المثال- ضحية لمثل هذا النمط من الافعال الاجرامية غير المشروعة.

ب- الابقاء على مستخدمين تركوا الوظيفة بالفعل:

ويتلخص هذا النمط من افعال الغش المعلوماتى، فى أن المبرمج المسئول عن الادارة المعلوماتية بدلامن أن يحفظ ملفات الاشخاص الذين تركوا العمل بالمنشأة، فانه يبقى هذه الملفات على قيد الحياة، ويجعلها تدر دخلا لصالحة مع نهاية كل شهر.

ج-اختلاس النقود:

يرى الخبراء أن بامكان اى شخص يشغل مركزا على قدر من الاهمية فى احدى المنشآت أو الادارات أو المؤسسات أو البنوك، ولدية الكفاءة والخبرة الفنية اللازمة لاستخدام الحاسب الآلى، أن يغترف من هذا الاخير ما يشاء من معلومات يرغب فيها، بغية اختلاس العديد من المبالغ المالية والحاسبات الضخمة فى النهاية، منتهزا ضعف مراقبة الحاسب الآلى لمدى مشروعية هذا العمل وعدم قدرته على ذلك فى اغلب الاحيان:

ومن الامثلة على ذلك نذكر:

١- قيام شرطه مرسيليا الفرنسية بالقبض على مستخدم يعمل لدى فرع مصرف تابع لبنك Indo-Suez ، تمكن من عمل تحويلات لنقود وهمية مستخدما فى ذلك الحاسب الآلى الخاص بذلك البنك، وتلك المبالغ – ولو انها لم ترد فى الخزينة الخاصة بالبنك – الا انها قد سجلت فى ذاكرة الحاسب الآلى قبل أن تنتقل بواسطة محررات مصطنعة إلى حساب فتح باسمه فى سويسرا، وقد وجهت الاجهزة الامنية لهذا الشخص تهمة اختلاس سبعة ملايين فرنك فرنسى.

٢- فى فبراير من عام ١٩٨١ تم كشف قضية شهيرة جدا فى اسرائيل، تتلخص وقائعها فى أن شخصا يدعى Vladimir Loriblitt وهو مهاجر روسى عمل مبرجما فى وزارة المالية، وكان مولعا باصطناع الشركات الوهمية، قام بادخال فواتير وهمية لا حصر لها فى الحاسب الآلى، وقد سمح له ذلك أن يحول إلى تلك الشركات الوهمية العديد من الشيكات والمبالغ النقدية المسددة من T.V.A.

٢- اتلاف المعلومات الموجودة بالفعل فى الحاسب الآلى :

يمكن للمسئولين عن تخزين المعلومات وحفظها- وبمنتهى السهولة أن يغيروا ويتلفوا المعلومات المكلفين بحفظها داخل جهاز الحاسب الآلى، ومن الامور السهلة فى الواقع والتى تجسد تلك الافعال الاجرامية استبدال رقم حساب بآخر، أو احلال بطاقة محل اخرى، وهذا النوع من الجرائم على قدر كبير من الخطورة، لانه فى حالة نجاح التزوير، فانه يمكن لهذه الجرائم أن تستمر لفترة من الزمن حتى يتم كشف الفعل غير المشروع.

ومن الامثلة على ذلك نذكر:-

أ- استطاعت مجموعة من المستخدمين الاداريين خلال سنوات عديدة أن يضاعفوا من رواتبهم عن طريق استخدام الحاسبات الآلية، حتى لحظة الكشف عن تلك الافعال الاجرامية بمحض الصدفة.

ب- قام بعض المستخدمين الاداريين أيضا بتقاضى ساعات اضافية لم يتم تنفيذها على الاطلاق عن طريق استبدال قوائم الحاسبات بساعات عمل.

ج- امكن تقديم احد مرتكبى جرائم التزوير فى المعلومات للمحاكمة فى المانيا الشرقية (سابقا) ، حيث قام مستخدم بمكتب القوى العاملة- كان مكلفا بتوزيع الاعانات العائلية – بتحويل مبلغ وقدره ٥٠٠الف مارك المانى لحسابه الخاص فى شكل مرتبات، وقد نفذ ذلك عن طريق ازالة الرقم الاول لتلك المبالغ المحولة من المنفذ الخاص بمراقبة الحاسب الآلى ، وقد حكم عليه بالسجن لمدة ثلاث سنوات.

ج- لجأ بعض مرتبكى افعال الغش المعلوماتى الاكثر مهارة واحترافا إلى الهجوم المباشر على المعلومات المحمولة بواسطة شبكات الإتصالات البعيدة، وهم شديدو الولع بإلتقاط اذونات التحويل عن طريق وسائل الكترونية مصطنعة وتزويدها بالامر بدفع نفس المبلغ ولكن لحساب آخر.

ويتم اتلاف المعلومات أو تعديلها فى افعال الغش والتزوير المعلوماتى بوسائل متعددة ، نذكر منها:

أ- ممارسة **Bluff** : وتتجسد تلك الممارسة فى استخدام الحاسبات الإلكترونية من اجل طبع فواتير مصطنعة أو فواتير ذات قيمة كبيرة، ويقوم العملاء بتسديدها منخدعين فى الثقة التامة التى يتوسمونها فى تلك الحاسبات، والقليل من هؤلاء العملاء الذين يبدون اعتراضهم يتلقون خطابا تفسيريا مذيلا بصيغة صارت تقليدية ومالوفة وهى: (تقبلوا عذرنا، فقد اخطا حاسبنا الالى) وهكذا يستخدم الحاسب الآلى المتهم بسوء الادارة ككبش فداء ووسيلة سهلة لارتكاب تلك الأعمال غير المشروعة.

ب- التلاعب فى الاشرطة الممغنطة: اخفقت عملية نصب قدرت بحوالى ٢١ مليون فرنك فرنسى بسبب خطا لمعلوماتى مبتدئ وتتلخص وقائع تلك القضية فى انه بتاريخ ٢٩ فبراير ١٩٨١ وصل إلى أحد فروع الشركة العامة شريط ممغنط قادم من شركة **Isover st gobain** ، وقد احتوى هذا الشريط على ١٣٩ اذنا بالدفع، وعند معالجته بالقسم المعلوماتى للبنك تم رفضه بواسطة الحاسب الآلى نظرا لوجود عيب جسيم يتعلق بطول تسجيل هذا الشريط، وقد القى القبض على مرتكب هذه المحاولة الاحتيالية، وكان بالامكان – وفقا لراى الخبراء – أن يكتب لتلك المحاولة النجاح فى حالة المعرفة التقنية اللازمة فى المجال المعلوماتى لدى هذا المزيف .

ج- محو المعلومات: تمكن شخصان من اختلاس ٦١ الف دولار، وهى عبارة عن مبالغ مدفوعة مرسلة من شركات التأمين إلى احد المراكز الجامعية، ولكى يؤدى كل من هذين المحتالين عملهما الآثم على خير وجه، فقد قاما بمحو كل الحسابات القائمة فى تسجيلات الحاسب الآلى الخاص بذلك المركز الجامعى وجعلها غير قابلة للتحصيل.

وبالامكان أيضا أن تكون البيانات والمعلومات المعالجة آليا ليست فقط محلا للمحو الانتقائى، وانما أيضا للالغاء بلا قيد أو شرط، وهكذا ، فقد تم الكشف فى مدينة دالاس الامريكية عن اربعة من مستخدمى بلديتها، كانوا قد استبعدوا ٢٧١ مخالفة من سجلات المدينة مقابل تقاضى نسبة مئوية محددة بلغ مجموعها حوالى ١٦٣٠٠ دولار امريكى.

د- التلاعب فى المعلومات من بعد: يمكن أن تنفذ تلك الجرائم، فى حين يوجد مرتكبها على بعد عدة كيلومترات من مكان الاقتراف النهائى لها وتحقق نتيجتها الاجرامية، ويستطيع مرتكب فعل الغش المعلوماتى، هذا اذا ما تزود – على سبيل المثال- بكلمة السر أو مفتاح الشفرة أن يغير من ايه مسافة محتوى ومضمون ذاكرات الحاسبات الآلية وما يوجد عليها من بيانات أو معلومات، أو أن يستبدل ارقام حسابات بغيرها، ومن الامثلة على ذلك، أن طالبا امريكيا تدخل تدخلا غير مشروع فى احد النظم المعلوماتية ، واصبح مالكا له لفترة من الزمن، بعد أن قام بتغيير مفتاح الشفرة الخاص به، وترتب على ذلك أن رفض هذا النظام امداد اصحابة ومستخدميه الشرعين بالخدمات المعلوماتية لبضعة ساعات[٨٤].

ثانيا: التعدى على برامج التطبيق ونظم التشغيل:

يستلزم هذا النمط من الجرائم- وهو من جرائم المتخصصين والمحترفين – معرفة فنية دقيقة وعميقة فى مجال برمجة الحاسبات الآلية، وتنفيذه – وان كان من الصعوبة بمكان – الا انه يمكن أن يتحقق فى مراحل مختلفة من صنع برامج التشغيل أو التطبيق أو فى لحظة صيانتها أو تحديثها .

١- تعديل نظم أو برامج التطبيق:

يمثل هذا النوع من التعديل نسبة لا يستهان بها من افعال الغش والاحتيال المعلوماتى، واختلاس النقود فى معظم هذه الافعال كان هو الهدف والغرض المبتغى.

---

[٨٤]-أنظر : د/ محمد سامى الشوا ، ص٧١-٧٧.

ومن الامثلة على هذا التعديل والتى توضح مدى خطورة هذا النمط من الاجرام المعلوماتى نذكر:

أ- قيام مبرمج كان يعمل باحد البنوك بتعديل برنامج إدارة الحسابات فى هذا البنك، بحيث يضيف بموجب هذا التعديل ١٠ سنتات لمصاريف إدارة الحسابات على كل عشرة دولارات، ودولار واحد على الحسابات التى تتعدى عشرة دولارات، وقد تم قيد المصاريف الزائدة فى حساب خاص فتحة باسم مستعار، وهكذا فقد حصل هذا الجانى المختلس على عدة مئات من الدولارات كل شهر ، وكان بالامكان أن يستمر هذا العمل الاجرامى لولا أن البنك الذى كان يعمل به اراد بمناسبة تاسيس شركة جديدة للدعاية أن يكافئ أول واخر عميل له وفقا للترتيب الابجدى، وحينئذ اكتشف البنك عدم وجود هذا الاسم المستعار.

ب- اعد أحد المختلسين ويدعى Royce برنامجا للادارة المعلوماتية ، بحيث يسمح هذا البرنامج بادارة صحيحة لحسابات المنشأة، والتى تتضخم فى فترات زمنية ببعض النفقات ثم يقوم باستقطاع مبلغ زهيد من الايرادات كل شهر، وقد استطاع Royce أن يحقق فائدة على قدر كبير من الاهمية من خلال هذه الكسور المحسوبة بدقة والتى بلغ مقدارها حداً كبيراً ، وتمكن فى خلال ست سنوات من اختلاس مبلغ وقدره مليون دولار.

٢- تعديل نظم التشغيل:

يسمح نظام أو برنامج التشغيل – كما سبق القول – بتنظيم وضبط وتزامن توالى التعليمات والوظائف الخاصة بالحاسب الآلى ، وهناك اشكال متعددة لتعديل برامج التشغيل من اجل الحصول على مزايا غير مشروعه وتحقيق العديد من الاهداف الاجرامية، لعل اهمها:

أ- التعديل عن طريق المداخل المميزة:

يمكن أن يحتوى اى برنامج للتشغيل فى نسخته الاولى على اخطاء وعيوب منطقية، وقد لا يكتشف البعض منها الا عند استخدامه، ويمكن للمبرمجين عن طريق المداخل المميزة لتلك البرامج – والتى هى فى حقيقتها عبارة عن ممرات خالية متروكة فى البرنامج – احداث تعديلات فى شفرة هذا البرنامج والمنافذ الوسطية ، وتستبعد بالطبع هذه المنافذ عند التصحيح النهائى لبرامج التشغيل، وقد يصل الامر ببعض المبرمجين من ذوى النوايا السيئةو الاغراض غير المشروعه- والذين لهم دراية باهمية السلاح التقنى الموجود بين

ايـديهم- أن يتغاضـوا عـن اسـتبعاد هـذه المـداخل المميـزة ولا ينبهـوا اليهـا اى شخص، ونظرا لكونهم هم المؤتمنين فقط على هذا السر، فانـه يمكنـهم فى لحظـة معينـة أن يستخدما تقنيـة معلوماتيـة تتخذ من بـرامج التشـغيل هدفا لهـا ويطلـق عليها اصطلاح "Trappe" اى المصيدة ووفقا لهواهم، ويستمرون تبعا لذلك فـى استغلال برنـامج التشـغيل المعيب مـن الناحيـة الفنيـة، وبالامكـان أيضـا عـن طريـق هـذه المـداخل المميـزة الولـوج فـى كـل المعلومـات التـى تحتويهـا ذاكـرات الحاسبات الآلية، ومن ثم التوصل إلى الشفرات والتعليمات المستهدفة.

واجمالا، فانه يمكن عن طريق هذه الوسيلة أن يصبح مرتكب فعل الغش هو سيد النظام المعلوماتى ، مع ما يترتب على ذلك من نتائج ايجابية بالنسبة لـه، ونتـائج سـلبية مـع مزيـد مـن الخسـائر الفادحـة بالنسـبة لصـاحب أو المسـتخدم الاصلى للحاسب الآلى المسلوب.

ب- اصطناع برنامج:

يقصد الخبراء المعلوماتيون بلفظى" تصنيع وتشكيل" استخدام الحاسب الآلى من اجل التخطيط للجريمة ومراقبتها وتنفيذها , اى اصطناع برنـامج كامل ومخصص فقط لارتكاب فعل الغش المعلوماتى، والمثال الذى يساق عادة- بمنابـة هذا النمط من الغش المعلوماتى – من قبل بعض المتخصصين، هو ذلك الخـاص بشركة تـأمين بولايـة لـوس انجلـوس الامريكيـة، والتـى اختلقت بفضل حاسـبها الآلـى ومعاونـة مبرمجيهـا عددا وهمياً مـن المـؤمن عليـهم بلـغ حـوالى ٦٤ الـف وثيقة تأمين وقد تقاضت تلك الشركة من اتحاد شركات التأمين بالولايات المتحدة الامريكية عمولة نظير اجمالى تلك الوثائق (٦٤ الف وثيقة) واقتصر دورها فقط علـى إدارة الحسـابات ، وامعانـا فـى التضـليل، وبغـرض اعطـاء العقـود لاوهميـة مظهـراً مشـابها لتلـك الحقيقيـة، فقـد قامـت الشـركة المـذكورة بتنشـيط الملفـات المختلفة عن طريق تغيير الموطن والوظيفة وبعض الاقرارات الاخرى.

المطلب الثانى
التزوير المعلوماتى

يقصد بالتزوير- وفقا للراجح من أقوال الفقه- " كل تغيير للحقيقة مقترن

بقصد الغش يقع فى محرر باحدى الطرق التى نص عليها القانون ويكون من شانه أن يسبب ضررا للغير"[٨٥].

وبالنظر إلى المحررات فى نطاق المعلوماتية، فإننا نلاحظ أن الاعتماد على مستخرجات الحاسب الآلى من مستندات معلوماتية تخرج من الطابعة على هيئة اوراق أو شرائط ممغنطة مسجل عليها المعلومات قد بات ضرورة ملحة فى عصرنا الحالى، فجميع الإدارات والهيئات الحكومية والمدنية والتجارية أصبحت تعتمد – كما سبق أن بينا- على تلك الآلة الالكترونية فى تسيير شئونها المختلفة، وكذلك ايضا فى المحلات التجارية والفواتير المحاسبية فى جميع المجالات [٨٦].

ومن تحليل عناصر جريمة التزوير المادية، " فإننا نجد أن تغير الحقيقة الذى يقوم به التزوير هو فحسب الذى يقع فى محرر، لذلك لايعد تزويراً تغيير الحقيقة الذى يقع دون كتابة- بقول أو فعل- " كإدلاء شخص بأقوال كاذبة امام المحكمة، أو العبث فى العدادات الحاسبة(كعداد السيارة الاجرة وعدادات الكهرباء والغاز والمياه)، وإن جاز أن تقوم بتلك الافعال جريمة اخرى كشهادة الزور أو النصب أو الغش فى المعاملات، والمحرر فى جوهره كتابة مركبة من حروف أو علامات تعبر عن معنى أو فكرة معينة, وإمكانية القراءة البصرية للمدون به هو ما تفترضه نصوص التزوير التقليدية فى اغلب دول العالم، ويترتب على ذلك أنه لا ينطوى تحت هذه النصوص البيانات المخزنة إلكترونيا، فهذه البيانات- سواء كانت مخزنة فى ذاكرة الحاسب الآلى، ام متضمنة فى برامجة أو فى اشرطة الادخال أو الاخراج الممغنطة- ليست مقروءة ولا يمكن للمعنى الذى حمله أن ينتقل عن طريق عين الآدمى، إذ تسجل تلك البيانات على هيئة جزئيات دقيقة ومثبته الكترومغناطيسيا على دعامة تركيبية بشكل يسمح للحاسب فقط بقراءتها ، الامر الذى يتعذر معه اعتبارها محرراً، وهذا هو ما ذهب اليه عدد غير قليل من الفقة، وتطبيقا لذلك، لم تقر احدى محاكم الاستئناف بالولايات المتحدة (فى قضية U.Sv. Jones) حكما اصدرته محكمة المقاطعة بادانة شخص عن جريمة تزوير لقيامه بتحريف بيانات حسابات المدفوعات وادخالها فى نظام معلومات الحاسب الآلى الذى عالجها واصدر فى مخرجاته

---

[٨٥]- تعريف الاستاذ جارسون السائد فى الفقة الفرنسى لجريمة تزوير المحررات والذى درج الفقة فى كل من فرنسا ومصر على استعماله والأخذ به ، د. أحمد حسام طه تمام، ص ٣٨٦- ص ٣٨٧ ، د. هشام محمد رستم، ص ٣٢٣.

[٨٦]-أنظر : د/ أحمد حسام طه تمام، ص ٣٨٧- مرجع سابق .

خمس شيكات بمبلغ ١٣٠ ألف دولار قابلة للدفع فى حساب وهمى، وفى تسبيبها للحكم السابق ، قررت تلك المحكمة " أن ثمة فارقا بين محرر مزور ومحرر دون بـه مـا يخـالف الحقيقـة دون أن يتعرض مضمونه لتحريف (محرر صحيح فى تنفيذه واخراجه) ، وان افعال المتهم لاتشكل اصطناعا أو عملاً لمحرر مزور، وانه إذا كان من رأى محكمة المقاطعة أن الواقعة لا يستفاد منها أن الشيكات – بما سطر عليها من بيانات تغير الحقيقة- قد صدرت من الشركة المجنى عليها إلى الحساب الوهمى، فان المحكمة الاستئنافية لا تقرها فى ذلك ، لأن الشيكات – بما أثبت فيها من قابلية المبلغ المعين بها للدفع لامر الشخص الوهمى– تتضمن وجود التزام على عاتق المجنى عليه لصالح المستفيد، ومع أن هذا الالتزام لم يكن له بالقطع وجود ، إلا أن ما وقع من غش قد أفضى إلى اعتقاد المجنى عليه بأن على عاتقة التزام حقيقى تجاه هذا الشخص الوهمى، وهو ما تم بناء عليه إصدار صك أو مستند حقيقى أو اصلى متضمنا ما يغاير الحقيقة كما لو كان قد صدر لدائن فعلى".

على أن رأيا آخر، يدافع عنه جانب من الفقة البلجيكى والمصرى، يذهب إلى أن التغيير الذى يقع فى برامج الحاسب الآلى أو فى البيانات والمعلومات المخزنة إلكترونيا يمكن أن تتحقق به فى بعض الحالات جريمة التزوير فى المحررات، ويشير انصار هذا الراى إلى أن الفقة الحديث يقبل ذلك بالنسبة للاوراق المقواة المثقبة، وان ثمة تطوراً حدث بالفعل بشان المعلومات المسجلة على الاسطوانات والاشرطة الممغنطة ينحو إلى تطبيق نص التزوير فى المحررات على تحريفها، ويرى أحد الفقهاء المصريين أن البرنامج متى دون على اسطوانة أو شريط ممغنط يعتبر محرراً، وتغيير الحقيقة فيه يعد بالتالى تزويرا، ويعيب هذا الراى- عدم اتساقة مع المفهوم المستقر عليه فقها وقضاء لمدلول المحرر ، إذ يفترض هذا المفهوم أن المعنى الذى تعبر عنه الرموز أو العلامات المدونة بالمحرر ينتقل إلى الشخص بالنظر، وهو ما لا يتحقق فى البرامج المعلوماتية أو البيانات المخزنة إلكترونيا ، لانها تسجل كهرومغناطيسيا على الاسطوانات أو الاشرطة الممغنطة، فلا يمكن مشاهدتها فى ذاتها والتعرف عليها عن طريق النظر، كما أن من عناصر المحرر أن يدل بذاته على من ينسب اليه ، هو ما لا يتحقق كذلك فى برامج الحاسب الآلى.

من أجل ذلك حاول رأى ثالث التوفيق بين هذين الاتجاهين، معتبرا أن نصوص التزوير التقليدية فى المحررات من الممكن أن تنطبق فى حالة ظهور المعلومات والبيانات المزورة فى المخرجات الورقية للحاسب الآلى، وقد تبنى

هذا الاتجاه بعض الفقة فى كل من بجليكا وفرنسا ومصر، ففى فرنسا من المستقر فقها وقضاء أن الشرط الاول لقيام جريمة التزوير فى المحررات هو أن تكون هناك كتابة .. ومن ثم فان تغيير الحقيقة الذى يقع فى الاشرطة الممغنطة لا تقوم به جريمة التزوير فى المحررات المنصوص عليها فى المادة ١٤٥ من قانون العقوبات الفرنسى وما بعدها، وذلك لانتفاء الكتابة، غير أن هذه الجريمة يمكن أن تقع فى حالة إخراج الحاسب الالى أوراقا لها قوة أو قيمة فى الاثبات، كما هو الحال بالنسبة للمستند المحاسبى المزور أو الفاتورة المزورة) وفى مصر ، يرى البعض من الفقه أنه (يجب أن تكون الكتابة فى المحرر مركبة من حروف، وإن لم تكن من نوع الحروف المعروفة، مثل الكتابة المختزلة والشفرة السرية، وهذا ما ينطبق على البيانات الموجودة فى الحاسبات الآلية على الذاكرة والمعالجة آليا، فهى عبارة عن لغة خاصة بالحاسب الآلى وموجات هرتزية، فاذا وقع اعتداء عليها بتغير الحقيقة فإنه يكون اعتداء على البيانات وليس تزويرا، الا إذا خرج فى صورة محرر مكتوب بعد المعالجة الآلية للمعطيات الموجودة بالداخل والتى تم الاعتداء عليها"[٨٧].

وازاء هذا الخلاف فى الفقه والقضاء حول مدى جواز تطبيق النصوص التقليدية على الافعال التى تشكل تغييرا للحقيقة فى البيانات المخزنة إلكترونيا فى الحاسب الآلية والى يتحقق بها الركن المادى لجريمة التزوير المعلوماتى، وازاء ضيق نطاق تلك النصوص وعجزها- حسب الراجح فى الفقه والقضاء – عن مواجهة التزوير الذى يقع فى مجال المعالجة الإلكترونية للبيانات، وحماية للثقة الواجب توافرها فى المستندات المعالجة إلكترونيا- سيما بعد تعاظم الاعتماد عليها فى تسيير شئون المجتمع الحديث– فقد عمد المقنن فى العديد من الدول إلى ادخال هذه النوعية المستحدثة من التزوير فى دائرة التجريم والعقاب بمقتضى نصوص خاصة سنها لهذا الغرض ، أو بتعديلات أدخلها على بعض النصوص التقليدية للتزوير[٨٨].

[٨٧]-أنظر : د/ هشام رستم ، ص ٣٢٦- ص ٣٣٠. د. أحمد حسام طه تمام، ص ٣٩١.

[٨٨]-أنظر : د/ هشام رستم ، ص ٣٣١، ٣٣٢.

المطلب الثالث
النصب المعلوماتى

يقصد بالنصب "الاستيلاء على حيازة مال الغير الكاملة بوسيلة يشوبها الخداع تسفر عن تسليم ذلك المال"، ويتميز النصب عن السرقة – رغم تماثلهما فى الموضوع والغاية- فى أن الاستيلاء على الحيازة الكاملة للمال يتم فى السرقة بغير رضاء حر من مالك أو حائز هذا المال ، بينما يحصل فى النصب بتسليم مشوب بالاحتيال[٨٩] عن طريق استعمال الجانى لإحدى الطرق الاحتيالية التى ينص عليها نص التجريم عادة فى جريمة النصب، كما عرفة بعض الفقة بأنه" الاستيلاء بطريق الإحتيال على شئ مملوك للغير بنية تملكه" ، أو هو " الاستيلاء على منقول مملوك للغير بخداع المجنى عليه وحمله على تسليمة"[٩٠].

ومن الممكن أن يكون الحاسب الآلى احد وسائل الجانى فى ارتكاب جريمة النصب، ويطلق على جريمة النصب فى هذه الحالة اصطلاح " النصب المعلوماتى"، ولعل خير مثال للطرق الاحتيالية المستخدمة فى النصب المعلوماتى هو التلاعب المعلوماتى، والذى يقصد به" التلاعب بالبرامج والبيانات للتغيير فيها بما يترتب عليه ايهام المجنى عليه بصحتها بما يجعله يسلم بها"[٩١]، فجريمة النصب المعلوماتى تبدو من الوضوح بمكان فى الحالات التى يتوصل فيها شخص عن طريق التلاعب فى منظومات المعالجة الإلكترونية للبيانات إلى الاستيلاء على مال الغير، كأن يتلاعب فى البيانات المدخلة أو المخزنة داخل الحاسب أو فى برامجة لاستخراج شيكات تدفع له، أو لتحويل كل أو بعض ارصدة الغير أو الفوائد المستحقة لهم إلى حسابه، أو التلاعب فى الاشارات الإلكترونية المرتدة من الحاسب المركزى إلى جهاز الصرف الآلى للنقود لاختلاس أموال من ارصدة العملاء أو من رصيد جهاز الصرف نفسه دون

---

[٨٩]- أنظر : د/ حسن صادق المرصفاوى، قانون العقوبات الخاص، منشاة المعارف، الاسكندرية، ١٩٩١، ص ٣٩٤، د. هشام محمد فريد رستم، ص ٢٦٨

[٩٠]- أنظر : د/ هشام محمد فريد رستم، هامش (١) ، ص ٢٦٨

[٩١]- أنظر : د/ هدى حامد قشقوش ، جرائم الحاسب الالكترونى فى التشريع المقارن، دار النهضة العربية، القاهرة، ١٩٩٢، ص ١٣٢.

التأثير فى بيانات الحاسب المركزى وفى حسابات العملاء[٩٢]، كما يمكن ايضا استخدام الحاسب الآلى بهدف التزييف أو التزوير، وحالة الفواتير المزورة هى المثال الواضح على ذلك ، وفى الواقع فانه يوجد فى هذه الحالة مستندات من مستخرجات ناتجة عن استخدام الحاسب الآلى تكون ذات طبيعة من شانها الايهام بوجود أموال وهيمة، وذلك بسبب اعدادها بطريقة الكترونية وحسابية من شانها الإيحاء بوجود قوة واموال، وذلك فى الحالة التى تكون عليها الوثيقة مستخرجة من الحاسب الآلى، ويرجع ذلك للثقة التى يعطيها الاشخاص للوثائق المستخرجة من الحاسبات الالية[٩٣].

كما يمكن كذلك استخدام الحاسب الآلى فى ارتكاب جرائم النصب المعلوماتى عن طريق احدى الوسائل التدليسية" كاستخدام صفة غير صحيحة أو اسم كاذب" والدليل الواضح على ذلك هو استعمال الكارت الائتمائى أو البطاقة البنكية الممغنطة باسم كاذب أو بصفة كاذبة[٩٤]، " وتعتبر الجرائم المتعلقة باساءة استخدام البطاقات البنكية الممغنطة أو الكروت الائتمانية الممغنطة من الجرائم المقلقة خصوصا فى المجتمعات التى تتسم نظمها البنكية بدرجة عالية من التطور والحداثة، وتمنح فيها البطاقات الائتمانية وتستخدم كذلك باقل قدر ممكن من الاجراءات، ففى وقتنا الحاضر اصبح فتح الحساب البنكى أو الائتمانى فى اغلب دول العالم من الحقوق التى اعترف بها القضاء للناس كافة، بل أن فتح حساب بنكى اصبح من الامور الواجبة، كما فى حالة لو كان الموظف أو العامل يحصل على مرتبة أو اجرة من خلال احد البنوك، وقد نتج عن ذلك أن اصبح الحصول على احدى البطاقات البنكية من الامور المرتبطة بأحقية الفرد فى فتح حساب بنكى،ومنح البطاقة الائتمانية يتم من قبل البنك باسم الشخص وان صغرت قيمة ودائعة، وكما أن دفاتر الشيكات يتم الحصول عليها بسهولة ، فكذلك الحال بالنسبة للبطاقات الائتمانية أو البنكية، فهى تستخدم كذلك بنفس السهولة فى تسوية المدفوعات التى يقوم الفرد بها نظير الشراء والحصول على الخدمات المختلفة من التجار وغيرهم ، ومهما كانت قيمة هذه المدفوعات سواء قلت ام كثرت، وتتعدد صور اساءة استخدام البطاقات البنكية، ولعل من اشهر تلك الصور (جريمة استخدام البطاقات المسروقة أو منتهية الصلاحية، وجريمة تزوير

---

[٩٢]-أنظر : د/ هشام محمد فريد رستم، ص٢٦٩- ٢٧٠

[٩٣]-أنظر : د/ احمد حسام طه تمام، ص ٢٠٩- ٢١٠.

[٩٤]-أنظر : د/ هدى حامد قشقوش ، المرجع نفسه ، ص ١٣٢- ١٣٣.

البطاقات الحقيقية، وصورة قيام صاحب البطاقة ذاته بسحب مبالغ نقدية اكبر من المبالغ المسموح له بسحبها من آلة التوزيع الآلى للنقود مستغلاً بذلك بعض الثغرات التى ما زالت هذه الآلات تعانى منها حتى الآن)، وتتنوع كذلك طرق تنفيذ جريمة سحب مبالغ نقدية أكبر من المبالغ المسموح بسحبها من آلة التوزيع الآلى للنقود، فبعض حاملى البطاقات البنكية يكتفون باستخدام تلك البطاقة فى سحب مبالغ اكثر مما ينبغى لهم سحبة، والبعض الآخر وهم الاكثر خطورة يقومون بابلاغ البنك بضياع بطاقتهم الائتمانية- دون أن يكون ذلك صحيحا- ثم يقومون على الفور، وقبل أن يقوم البنك بالتحفظ على اموالهم وحمايتها، باستخدام البطاقة المبلغ عن ضياعها فى سحب مبالغ معينة من حساباتهم البنكية، بحيث يعطوا انطباعا بان سارق البطاقة أو من وجدها هو الذى قام بسحب تلك المبالغ النقدية[٩٥].

المطلب الرابع
جرائم الاعتداء على حرمة الحياة الخاصة

أهمية البيانات والمعلومات المتعلقة بالحياة الخاصة والمخزنة الكترونيا

لحياة الافراد خصوصيتها بما تحوية من اسرار وخصوصيات ، والمحافظة عليها من اكثر الامور التى تحظى بحماية دستورية وقانونية فى كافة دساتير العالم المتمدين وقوانينها"[٩٦].

" ولئن كان صحيحا ما لاحظة بعض علماء الاجتماع من أن ثمة ارتباطا وثيقا بين التقدم التقنى واتساع نطاق الرقابة الاجتماعية على الافراد ، فان هذه الرقابة قد بلغت منتهاها مع تسارع وتيرة تقدم تقنية الحاسبات الآلية واطراد الاعتماد عليها فى تسيير شئون المجتمعات، اذ تتيح تلك الآلات الإلكترونية امكانات فائقة لتخزين ومعالجة واسترجاع ونقل كم هائل من البيانات والمعلومات التى تقوم الدول الحديثة بجمعها عن الافراد، وهو ما يجعلها – حسب وصف بعض الفقه- اداة للرقابة غيرمسبوقة فى يد السلطات، اضف إلى ذلك أن كثيرا

[٩٥]-أنظر : د/احمد حسام طه تمام، ص ٢١٠- ٢١١

[٩٦]-أنظر : د/ أحمد حسام طه تمام، ص ٣١٥

من المؤسسات الكبرى والشركات الحكومية والخاصة تجمع عن الافراد بيانات عديدة ومفصلة تتعلق بالوضع المادى أو الصحى أو التعليمى أو العائلى أو العادات الاجتماعية أو العمل.. الخ.

وتستخدم الحاسبات الآلية وشبكات الاتصال والمعلومات فى خزن تلك البيانات الخصوصية ومعالجتها وتحليلها والربط بينها واسترجاعها ومقارنتها ونقلها، وهو ما يجعل فرص الوصول إلى هذه البيانات على نحو غير مصرح أو ماذون به أو بطريق التحايل اكثر من ذى قبل، ويفتح مجالا اوسع لاساءة استخدامها أو توجيهها توجيها منحرفا أو خاطئاً أو مراقبة الافراد وتعرية خصوصياتهم أو الحكم عليهم حكما خفيا من واقع سجلات البيانات الشخصية المخزنة، الامر الذى حدا بكثيرين إلى وصف استخدام الحاسبات الآلية كبنوك للبيانات والمعلومات بانه تهديد غير مقبول للخصوصية والحريات المدنية.

وفى ثناياها، تحمل تلك الحاسبات نفس المخاطر المهددة للخصوصية التى عرفتها البشرية فى مجال النظم اليدوية لتسجيل وحفظ واسترجاع البيانات الشخصية، غير انها تضيف اليها ابعادا جديدة وخطيرة نابعة من طبيعة تلك الآلات التقنية المتقدمة فى مجالات تخزين البيانات والمعلومات ومعالجتها ونقلها.

ففى مجالات التخزين، نجد أن التقدم العلمى لا يصادف اية عقبات فنية، ولذلك فان سعة ذاكرات الحاسبات الآلية غير محدودة علميا، ووسائط أو اوعية المعلومات يتزايد على الدوام حجم تخزينها للبيانات والمعلومات مع صغر وتضاؤل شكلها الخارجى، ومن شان ذلك انشاء بنوك أو مراكز وطنية للمعلومات تخزن فيها الدولة ملفات تحتوى معلومات شاملة ومفصلة عن الافراد، وهو ما حدث بالفعل فى دول العالم المتمدين، وتكمن فى هذه المراكز والبنوك اكثر التهديدات جسامة لحرمة الحياة الخاصة للافراد، ففى هذه البنوك يمكن تخزين اكبر قدر ممكن من المعلومات عن ملايين الاشخاص، والاحتفاظ بها إلى الابد، واستخراج بيانات كافية عن اى انسان من المسجلين بها، وتعرية حياته بكشف تفاصيل سابقة على وقت استخراج تلك البيانات بزمن طويل، مما قد يسبب له اضرارا بليغة يتعذر أو يستحيل اصلاحها وتداركها، فضلا عن أن هذه المعلومات

الشخصية تصبح فى هذه البنوك مجمعة، متوافرة، سهلة المنال ومتاح استخدامها فى اغراض الرقابة على الافراد والاشخاص الطبيعية والمعنوية على حد سواء.

وفى مجالات معالجة البيانات تتجلى المخاطر التى تهدد حرمة الحياة الخاصة للافراد عند ربط الحاسبات بعضها ببعض أو ربطه بحاسب مركزى أو بشبكات عامة للاتصالات و المعلومات ، حيث يتسنى بذلك تبادل المعلومات فيما بين المراكز المعلوماتية المتباعدة مكانيا والمختلفة من حيث اغراض تخزين البيانات بها، وربط هذه المعلومات بعضها البعض واستكمالها وتحليلها ومعالجتها على نحو يتيح التوصل إلى معلومات جديدة عن شخص أو مجموعة اشخاص.

واخيرا ، وفى مجالات نقل البيانات و المعلومات: يلاحظ أن المخاطر المهددة للخصوصية تظهر بشكل واضح وجلى فى عدم قدرة شبكات الاتصال على توفير امان مطلق أو كامل لسرية ما ينقل عبرها من بيانات ومعلومات، وامكانية استخدام هذه الشبكات فى الحصول بصورة غير مشروعة من بعد على المعلومات"[٩٧].

صورة الانتهاكات المعلوماتية الواقعة على حرمة الحياة الخصوصية

لعل من اخطر الجرائم التى يمكن أن تقع عن طريق الحاسبات الآلية وشبكات الاتصالات و المعلومات الخاصة بها (الإنترنت) هى جرائم الاعتداء على حرمة الحياة الخاصة، نظرا لعدم وجود الحماية التقنية الفاعلة والفعالة فى نفس الوقت لما يتم تداوله من بيانات ومعلومات واسرار ومراسلات بطريقة الحاسبات الآلية والانترنت[٩٨]، وللانتهاكات المعلوماتية لحرمة الحياة الخاصة صور واشكال تمارس من خلالها العديد من الاعتداء على الاسرار المعلوماتية المتعلقة بالافراد والاشخاص وخصوصية حياتهم، ولعل من ابرز تلك الصور ما يلى:

---

[٩٧]-أنظر : د/ هشام محمد فريد رستم ، ص ١٧٨- ١٨٤

[٩٨]- أنظر : د/ مدحت رمضان، جرائم الاعتداء على الاشخاص والانترنت، دار النهضة العربية- القاهرة- ٢٠٠٠ – صفحة ١٠١.

اولا: استخدام بيانات شخصية غير صحيحة:

ويتحقق ذلك فى احد شكلين، هما:

١- التلاعب فى البيانات الشخصية أو محوها من قبل اشخاص غير مصرح لهم بذلك.

٢- جمع أو معالجة أو نشر بيانات شخصية غير صحيحة من قبل الاشخاص المرخص لهم بذلك قانونا :

١- التلاعب فى البيانات الشخصية أو محوها من قبل اشخاص غير مصرح لهم بذلك.

ويقترن هذا التلاعب أو المحو عادة بتحقيق مصالح مالية للجناة، إلى جانب انتهاكة للسرية وحرمة الحياة الخاصة للافراد، ويمكن الاشارة فى هذا الخصوص إلى حالة واقعية حدثت فى شركة TRW company credit data الامريكية، وتخلص وقائع هذه القضية فى أن هذه الشركة كانت تزود عملاءها (وكان اكثرهم من البنوك والمتاجر الكبرى وشركات تسهيلات الائتمان وشركات تاجير السيارات والمعدات الثقيلة) من خلال حاسباتها وانظمتها المعلوماتية بمعلومات تتعلق بالمركز الائتمانى للاشخاص الذين يرغب هؤلاء العملاء فى التعامل معهم، وذلك تجنبا للمخاطر التى قد تترتب على التعامل مع اشخاص لا يتمتعون بمركز ائتمانى جيد، وكانت الشركة تقدم هذه الخدمة نظير اشتراك يدفعه العملاء، وذلك من واقع بيانات عن اشخاص (بلغ عددهم سنه ١٩٧٦ حوالى ٥٠ مليون شخص) كانت الشركة تقوم بجمعها وحفظها فى الملفات المخزنة بحاسباتها الآلية، وقد اغرى هذا النشاط ستة من العاملين بتلك الشركة- من بينهم كاتب بقسم علاقات المستاجرين – على الاتجار فى هذا النشا والتلاعب فى هذه البيانات عن طريق تعديل أو محو البيانات التى تظهر المركز الائتمانى السيئى لصاحبها لتحل محلها بيانات جديدة تفيد تمتع صاحبها بمركز ائتمائى جيد، وذلك فى مقابل مبالغ ماليه تم الاتفاق عليها، وبناء على هذه البيانات الائتمانية الزائفة التى تم إدخالها بالمحو أو الاضافة أو بهما معا إلى نظام معلومات حاسب شركة TRW، فقد تورط العديد من عملائها فى معاملات مالية وتجارية مع اشخاص ذوى سمعة ائتمانية سيئة، وقد قدر البعض عدد السجلات التى تم التلاعب فى بياناته باكثر من مائة سجل ، رغم أن الادعاء العام قام بتسجيل ست عشرة حالة تزوير فقط، وكشأن اكثر الجرائم المعلوماتية ، فان امر الجناة فى تلك القضية لم يكتشف الا عرضا، إذ اتصلوا بأحد الاشخاص

عارضين عليه تعديل البيانات الائتمانية الخاصة به مقابل ٦٠٠ دولار يدفعها، فاستشاط غضبا وقام بابلاغ مكب التحقيقات الفدرالية FBI، وفى التحقيقات اعترف كاتب قسم علاقات المستهلكين تفصيليا وشهد على ما قام به شركاؤه.

٢- جمع أو معالجة أو نشر بيانات شخصية غير صحيحة من قبل الاشخاص المرخص لهم بذلك قانونا :

وهذه هى الطريقة الثانية التى يتم من خلالها استخدام بيانات شخصية غير صحيحة، حيث تنصب أفعال الجمع أو المعالجة أو النشر التى يأتيها المصرح لهم بذلك من قبل القانون على بيانات ومعلومات مزورة أو غير صحيحة، وقد يتم ذلك كله بصورة عمدية، حينما يكون إرتكاب هذه الافعال والانتهاكات مصحوبا بالعلم بمخالفة البيانات الشخصية للحقيقة وكونها غير صحيحة مع إرادة جمعها أو معالجتها أو نشرها، الا أن كثيرا من حالات جمع أو معالجة أو نشر البيانات و المعلومات الشخصية غير الصحيحة انما يتم عن طريق الاهمال وبوجه خاص فى نطاق نظم تقارير الائتمان.

ثانيا: جمع أو تخزين بيانات شخصية صحيحة ولكن على نحو غير مشروع جنائيا:

لا يتم انتهاك الخصوصية وحقوق الافراد الشخصية فى مجال المعلوماتية- فقط – عن طريق استخدام بيانات ومعلومات شخصية غير صحيحة، وانما قد يتم ذلك ايضا عن طريق جمع أو تخزين بيانات شخصية صحيحة فى ذاتها ولكن على نحو غير مشروع جنائيا، وصفة عدم المشروعية الجنائية التى تلحق افعال الجمع أو التخزين فى هذه الحالة قد يكون مصدرها الاساليب غير المشروعة المستخدمة للحصول على هذه البيانات و المعلومات، وقد يكون مصدرها ايضا مضمون هذه البيانات ذاته.

١- عدم مشروعية اساليب وطرق جمع أو تخزين البيانات والمعلومات:

يعتمد فى الحصول على البيانات والمعلومات على عدد من الاساليب التى يمكن استخدامها، والتى تشكل انتهاكا واضحا للخصوصية، ومن بين تلك الاساليب التقاط الارتجاجات التى تحدثها الاصوات فى الجدران الاسمنتية للحجرات وترجمتها ومعالجتها بحاسب آلى مزود ببرنامج خاص لترجمتها إلى كلمات وعبارات، أو مراقبة واعتراض والتقاط وتفريغ الرسائل المتبادلة عن طريق البريد الالكترونى، أو توصيل اسلاك بطريقة خفية إلى الحاسب الآلى الذى تخزن داخله البيانات المطلوب الاستيلاء عليها، أو التوصل بطريق غير مشروع

إلى ملفات بيانات تخص الاخرين، ومما لاشك فيه أن الزيادة المستمرة فى استخدام الحاسبات الشخصية والبريد الالكترونى وشبكات الاتصالات ونقل البيانات والمعلومات عن بعد سوف تؤدى حتما إلى زيادة استعمال هذه الاساليب غير المشروعة، والى تفاقم الاضرار والخسائر الناتجة عنها.

وقد اشار الاستاذ Sieber إلى حالة واقعية استخدمت فيها طريقة ماسة بحرمة الحياة الخاصة للحصول على بيانات شخصية، وتتلخص هذه الحالة فى قيام مراهق من المانيا الاتحادية (سابقا) – لا يتجاوز عمره ستة عشر عاما- بنصب (مصائد بيانات) لالتقاط وجمع بيانات ذات طبيعة شخصية خاصة بمستخدمى انظمة الفيديوتكس Video Tex ، اضافة إلى قيامه بعمليات تلاعب واتلاف لبيانات بعض المستخدمين وتغيير كلمات السر التى يستخدمها بعضهم للتعامل مع النظام، مما ادى إلى حرمانهم من استخدامه[٩٩].

٢- عدم مشروعية مضمون البيانات التى يتم جمعها أو تخزينها:

البيانات والمعلومات ذات الطبيعة الشخصية متعددة ومتنوعة، ومن بينها زمرة أو مجموعة لا يفترض – نظرا لطبيعة مضمونها- أن يتم جمعها أو تخزينها، وتحديد نوعية البيانات التى تتألف منها هذه الزمرة هو احد ابرز الصعوبات التى تواجه حماية الحق فى الخصوصية، لان بالامكان استخدام الحاسبات الآلية فى معالجة بيانات شخصيةجزئية (كالبيانات الصحبة والتعليمية، والبيانات المتعلقة بمستوى وكيفية اداء الخدمة العسكرية، والعمليات البنكية، والمعاملات الضريبية، والتعامل ببطاقات الائتمان، وطلبات الاعانة التى تقدم لجهات حكومية، والتبرعات التى تقدم لجهات معينة، والاشتراك فى صحف معينة ونوعية الكتب التى يتم استعارتها من المكتبات العامة.. الخ) على نحو يتيح مراقبة الافراد وتحليل تصرفاتهم للتعرف على ابرز السمات المميزة لسلوكهم واستنتاج صورة تقريبية لشخصياتهم ، وهو ما يجعل حياتهم اشبة بكتاب مفتوح بمقدور اى شخص لدية امكانية التوصل إلى ملفات الحاسب الآلى قراءته، فعدم وجود ضوابط قانونية فى هذا المجال يؤدى إلى امكانية جمع وتخزين ونقل كم هائل من المعلومات قد تتعلق بأدق الامور الخاصة بالافراد، وهو ما قد يسمح بخلق صورة تفصيلية لشخصياتهم بمجرد الاطلاع على الملف الذى يحتوى على هذه المعلومات داخل نظام الحاسب الآلى.

[٩٩]-أنظر : د/ هشام محمد فريد رستم ، هامش (١) ص ١٩١

والواقع أن تحديد من له الحق فى جمع وتخزين البيانات من ناحية، ونوعية هذه البيانات من ناحية اخرى، هى واحدة من اهم الصعوبات التى تواجه حماية الحياة الخاصة فى مجال المعلوماتية ايضا.

ثالثا: الافشاء غير المشروع للبيانات الشخصية واساءة استخدامها:

تنقسم البيانات الشخصية التى تخزن فى ذاكرات الحاسبات الآلية وبنوك المعلومات من حيث الحماية التى يكفلها لها قانون العقوبات- وفقا لراى الاستاذ Sieber- إلى نوعين: " نوع يضم البيانات الشخصية السرية المشمولة بالحماية الجنائية التقليدية للاسرار، ونوع يضم ما عدا ذلك من بيانات شخصية غير سرية".

١- البيانات الشخصية السرية المشمولة بالحماية الجنائية التقليدية للاسرار:

تلحق صفة عدم مشروعية افشاء البيانات الشخصية فى الأحوال التى تسرى فيها على هذه البيانات النصوص الجنائية التقليدية المتعلقة بحماية الاسرار، ويبدو ذلك بوضوح فى مجالات عديدة، وعلى وجه الخصوص فى مجالات الطب والمحاماة والاعمال المصرفية، ومن قبيل ذلك الكشف عن شخصية صاحب الحساب أو الوديعة المرقمة، أو افشاء معلومات خاصة باحد الموكلين فى مكتب للمحاماة مخزنة على الحاسب الآلى الخاص بهذا المكتب والافصاح بها لمن ليس له حق الاطلاع عليها ومعرفتها ، وتبدو سمة عدم المشروعية واضحة ايضا فى حالة اساءة استخدام هذه البيانات والمعلومات باستخدامها فى غير الغرض الذى جمعت وخزنت من اجلة.

ولعل اكثر البيانات الشخصية السرية تعرضاً لخطر الافشاء غير المشروع هو المخزن منها فى ذاكرات الحاسبات الآلية للبنوك.

كما يتجلى ايضا هذا الافشاء للبيانات والمعلومات السرية فى القطاع الامنى والشرطى، حيث يتزايد الاعتماد على الأنظمة الإلكترونية فى تخزين ومعالجة ونقل البيانات المتعلقة بملايين الاشخاص، ومن الامثلة على ذلك ، ما ذكره الاستاذ Sieber، من قيام احد ضباط شرطة العاصمة النمساوية فيينا بتزويد مخبر خاص – خلال الفترة من عام ١٩٦١ حتى عام ١٩٧٨ – ببيانات السجلات الجنائية وملفات معلومات البحث الجنائى وملفات الشرطة الجنائية الدولية (الانتربول) المخزنة فى حاسب الشرطة عن بعض الاشخاص.

٢- البيانات الشخصية غير السرية:

من البيانات الشخصية ما يصعب- فى بعض الاحيان- اعتبار افشائه

محققا لضرر أو خطر على المجتمع يستوجب وصفة بأنه "غير مشروع جنائيا" أو" اجرامى" ، ويبدو ذلك بشكل واضح فى حالة المقارنة بواسطة الحاسب الآلى بين البيانات الشخصية المسجلة إلكترونيا لدى مختلف الاجهزة الحكومية بهدف ضبط الأداء وضمان حسن الادارة، وكشف الاحتيال الذى قد يمارسه البعض للاستفادة من المساعدات التى تقدمها هذه الاجهزة.

ويرى بعض الفقة أن برامج المقارنة الإلكترونية للبيانات تسهم فى ضبط الاداء بالنسبة للاجهزة الحكومية، وتحسين مستوى هذا الاداء، وضمان حسن تطبيق القانون، اضافة إلى انخفاض تكلفتها مقارنة بفاعليتها فى كشف الغش والاحتيال للحصول على المساعدات الحكومية بعيدا عن التعرض لخصوصيات المستفيدين، الا أن رايا اخر يعارض ذلك متخوفا، من امكانية استغلال هذه المقارنة لتحقيق اغراض لا تتعلق بكشف الغش والاحتيال ، أو أن يؤدى التمادى فى السعى لكشف ذلك إلى التغاضى عن التاثيرات السلبية لهذه المقارنة على السرية الشخصية والخصوصية ، ويقرر هذا الراى ايضا انه لئن كان ممكنا تبرير هذه المقارنة فى حالات فردية، الا أن التمادى فيها يظل قائما ومهددا بكشف الستار عن الاسرار والحياة الخاصة.

رابعا: مخالفة القواعد الشكلية المنظمة لجمع ومعالجة ونشر البيانات ذات الطبيعة الشخصية التى تدخل فى نطاق الحماية التشريعية لخصوصية المعلومات:

أن ضرورة حماية خصوصية المعلومات حتى فى الحالات التى اجيز فيها جمعها ومعالجتها ونشرها، قد دفع غالبية النظم القانونية الى وضع مجموعة من القواعد الشكلية لتنظيم جمع ومعالجة ونشر البيانات الشخصية، مثل ضرورة الحصول على ترخيص بذلك ، وفى كثير الدول يعد خرق هذه القواعد الشكلية جريمة يعاقب عليها القانون.

المطلب الخامس

جرائم الاعتداء على حقوق الملكية الفكرية والادبية

من الجرائم التى انتشرت ايضا – وبصورة خطيرة - فى الاونة الاخيرة،

جرائم الاعتداء على حقوق الملكية الادبية والفكرية بواسطة استخدام الحاسبات الآلية وشبكة الانترنت"، والاعتداء على الحقوق الادبية والفكرية أو ما اصطلح على تسميتة "بحقوق المؤلف" لا ينبغى الخلط بينه وبين الاعتداء على الملكية الادبية والفكرية التى تنصب على البرامج والمعلومات فى مجال المعلوماتية وتكنولوجيا المعلومات ، فهذه الاخيرة- الملكية الادبية والفكرية- تنصب على البرامج و المعلومات، اما الاعتداء على الحقوق الفكرية والادبية فهو يقع دائماعلى العناصر غير المادية لنظام المعلوماتية، "والمثال الواضح على استخدام الحاسب الآلى فى الاعتداء على الحقوق الفكرية والادبية هو استخدام ما يمنحه الحاسب من وسائل لخرق قواعد القانون المتعلقة بحقوق المؤلف . كما لو استخدم الحاسب الآلى فى السطو على بنوك المعلومات التى تتضمنها برامج حاسب آخر ، أو كما فى حالة تخزين هذه المعلومات على حاسب معين ثم يقوم المسئول عن هذا التخزين باستخدام هذه المعلومات أو التفريط فيها بدون اذن صاحبها".

والواقع أن استخدام معلومة معينة بدون اذن صاحبها يتضمن انتهاكا مزدوجا لحقوق هذا الشخص ، فهو من ناحية اعتداء على القيمة المالية التى قد تمثلها المعلومة، وهو من ناحية اخرى اعتداء على حق من الحقوق المعنوية على اعتبار أن للمعلومة قيمة ادبية علاوة على قيمتها المادية[١٠٠].

المطلب السادس
جرائم إفشاء الأسرار فى اطار المعلوماتية

قد تستخدم الحاسبات الآلية وشبكات الاتصال والمعلومات الخاصة بها فى ارتكاب العديد من الجرائم المتعلقة بافشاء الاسرار، والحاسب الآلى يعتبر بالفعل وسيلة فعالة فى هذا النوع من الجرائم نظراً لكونه آلة مستعدة تماماً لفتح ابوابها لمن يحسن إستخدامها.

والواقع أنه يمكن استخدام الحاسب الآلى فى ارتكاب انواع عديدة من هذه الجرائم أهمها:

١- إفشاء سرية المعلومات:

[١٠٠]-أنظر : د/ هشام رستم، ص ١٨٧- ص ٢٠١، د. نائلة عادل محمد فريد ، ص ٢٤٢- ص ٢٤٦.

قد تتخذ المعلومات صور المعاملات اليومية (كالخطابات والمحادثات الهاتفية) وتشكل هذه المعلومات قدراً كبيراً من المعلومات التى تحظى باهمية خاصة فى مجال تكنولوجيا المعلومات، وهو ما يتطلب حمايتها من الوصول اليها والتلاعب بها، ومما لا شك فيه أن افشاء سرية الاتصالات بما تشمله من خطابات ومحادثات هاتفية باعتباره صورة من صور المعلومة، قد يفضى إلى تدمير العديد من المؤسسات والمصالح بل وتعريض الدول ايضا واقتصادياتها لاضرار بالغة، نتيجة لاعتماد قطاعات مختلفة فى الدولة – فى تسيير شئونها – الحيوية - على سرية تلك الاتصالات والخطابات.

ولعل فى العبث فى شبكات الاتصالات والمعلومات الخاصة بالحاسب الآلى، وانتهاك العديد من مواقع البريد الالكترونى على شبكة الانترنت، ما ينبئ عن تفشى تلك الجرائم فى الحاضر والمستقبل القريب والبعيد على حد سواء.

٢- إفشاء اسرار الدفاع الوطنى والامن القومى:

قد تمس الجرائم المعلوماتية المصالح العليا للدولة، عن طريق افشاء العديد من الاسرار والمعلومات التى تتعلق بالامن القومى للدولة" كما لو كانت تتعلق بالمخابرات العامة أو بالدفاع الوطنى" ولاشك فى أهمية هذه البيانات والمعلومات المخزنة آليا وتأثيرها البالغ على مستقبل الدول والشعوب على حد سواء.

٣- إفشاء الاسرار المهنية:

يتوقف نجاح العديد من اصحاب المهن الحرة والمؤسسات والنشاطات على التكتم والاحتفاظ بالعديد من الاسرار المهنية واسرار العملاء فى حاسباتهم الآلية وعدم اطلاع الغير عليها، كما يقوم العديد من اصحاب المهن الحرة ايضا بتخزين بيانات ومعلومات تتعلق بادق تفاصيل واسرار حياة العملاء وتعاملاتهم فى حاسباتهم الآلية مع تعهدهم بالاحتفاظ بها وعدم اطلاع الغير عليها، ولاشك أن فى افشاء تلك الاسرار والمعلومات ما يعرض حياة العديد من الاشخاص ومصالحهم لاخطار واضرار بالغة.

٤- إفشاء الاسرار الصناعية:

وهناك اخيرا من المعلومات ما اطلق عليه " سر المهنة أو سر الصنعة"

فكثير من المشروعات المالية والاقتصادية والخدمية يتوقف نجاحها على مثل هذا السر الذى يميزها عن غيرها من جودة الانتاج أونى الإستنثارية ، كما أن من المعلومات ما يتعلق بخطوات ومراحل الانتاج الصناعى المختلفة ، فالسلعة أو الخدمة تمر بعدة مراحل متفاوته حتى تصل إلى شكلها النهائى الذى نراها عليه، وتعد هذه المراحل من المعلومات المهمة التى يحرص اصحاب الاعمال والمشروعات على الاحتفاظ بها وحمايتها من الاطلاع عليها من قبل الغير، ولا يخفى على احد حجم الاضرار الناجمة والمترتبة على الافشاء بأى من هذه المعلومات ذات الاهمية القصوى.

المطلب السابع
جرائم السب والقذف عبر الإنترنت

يقصد بالسب " كل تعبير يخدش الشرف والاعتبار" وقد عرفته محكمة النقض المصرية بانه "فى اصل اللغة الشتم سواء باطلاق اللفظ الصريح الدال عليه أو باستعمال المعاريض التى تومئ اليه ، وهو المعنى الملحوظ فى اصطلاح القانون الذى اعتبر السب كل الصاق لعيب أو تعبير يحط من قدر الشخص نفسه أو يخدش من سمعته لدى غيره "[١٠١]، [١٠٢].

اما القذف فيعرف بانه" الإسناد العلنى لواقعة محددة تستوجب عقاب أو احتقار من اسندت إليه" ، ويقصد بالاسناد " نسبة امر أو واقعة إلى شخص معين بأية وسيلة من وسائل التعبير عن المعنى"[١٠٣].

ويتميز السب عن القذف فى أن القذف لا يتحقق الا باسناد واقعة معينة يكون من شانها لو كانت صحيحة عقاب من اسندت اليه أو احتقاره بين اهل وطنه، اما السب فلا يستلزم أن يكون موضوع الاسناد واقعة معينة، بل يتحقق بالصاق أية صفة أو عيب أو معنى شائن إلى المجنى عليه[١٠٤].

---

[١٠١]- نقص ٢٨ يناير ١٩٨٥، مجموعة احكام النقض، س ٣٦، رقم ٢٥، ص ١٧٧.

[١٠٢]- د. على عبد القادر القهوجى، د. فتوح عبد الله الشاذلى ، شرح قانون العقوبات " القسم الخاص" ، دار المطبوعات الجامعية، الاسكندرية، ١٩٩٩، الكتاب الثانى" جرائم الاعتداء على الانسان والمال ، ص ٢١٥.

[١٠٣]- د.على عبد القادر القهوجى، د. فتوح عبد الله الشاذلى، المرجع السابق، ص ١٧٦.

[١٠٤]- د.على عبد القادر القهوجى، د. فتوح عبد الله الشاذلى، المرجع نفسه ، ص ٢١٥

والسب والقذف كلاهما من جرائم الاعتداء على الشرف والاعتبار، ويقصد بالشرف والاعتبار " المكانة الاجتماعية التى تحيلها الانسان فى مجتمعة والتى تتكون من مجموعة من الصفات الموروثه والمكتسبة، ومن علاقاته بغيرة من ابناء المجتمع، والتى يتحدد على اساسها مركزه الاجتماعى وما يستحق من احترام وتقدير بين مخالطية" وحق الانسان فى شرفة واعتباره من الحقوق اللصيقة بالشخصية القانونية والمتفرعة عنها ايا كانت المكانة الاجتماعية التى يحتلها فى المجتمع، وبالتالى لا يوجد شخص معدوم الشرف والاعتبار كلية منذ أن اعترفت القوانين الحديثة لكل فرد بشخصيته القانونية، والارتباط بين الشرف والاعتبار والشخصية القانونية- على هذا النحو – يسمح بالقول أن الاشخاص المعنوية- وليس فقط الشخص الطبيعى- لها الحق فى الشرف والاعتبار وتستحق ذات الحماية ما دام يعترف لها بالشخصية القانونية.

وهكذا فان شرف الانسان واعتباره يعتبر" قيمة اجتماعية" لا تقل اهمية عن تلك التى تتعلق بحق الانسان فى الحياة وفى سلامة بدنة، ومن ثم كانت جديرة باسباغ الحماية الجنائية عليها[١٠٥].

وفى إطار جرائم المعلوماتيه ، فاننا نجد العديد من افعال السب والقذف ترتكب على شبكة الانترنت، وبصفة خاصة على مواقع البريد الالكترونى والشبكة العالمية العنكبوتية (ويب) مع تزايد المنافسة غير المشروعة بين مختلف النشاطات فى اطار من حرية التجارة والحركة التى لا تحدها اية حدود، كما يزداد ارتكاب تلك الجرائم، ايضا بواسطة استخدام هذه الشبكات بغية التشهير والانتقام من العديد من الاشخاص والمؤسسات باقل السبل والتكلفة الممكنة، كما تكمن خطورة هذه الجرائم عند اختلاف وجهات النظر بين الدول والحكومات بصدد قضية أو مسألة معينة، فتعمد تلك الدول والحكومات إلى التشهير بغيرها من الدول الاخرى، والشعوب من خلال السيطرة على مؤسسات اعلامية تقوم ببث العديد من افعال السب والقذف والتشهير والتنكيل على مواقعها عبر شبكة الانترنت، بغية تضليل الراى العام بصدد تلك القضايا، أو التشهير والانتقام من الاطراف المعتدى عليها، والتى تراها تلك الدول والمؤسسات المسيطرة عليها عدوا لها من وجهة نظرها السياسية أو العنصرية، والمثال الواضح على ذلك ما

[١٠٥]- د.على عبد القادر القهوجى، د. فتوح عبد الله الشاذلى، ص ١٧٣

تقوم به بعض وسائل الاعلام التى تسيطر عليها الكيانات الصهيونية فى الدول الغربية من بث الروح المعادية للإسلام على شبكة الانترنت، وتضليل الراى العام فى تلك الدول وفى غيرها حول حقيقة الصراع العربى الإسرائيلى وماهية القضية الفلسطينية.

المطلب الثامن
الجرائم المخلة بالآداب العامة فى اطار المعلوماتية

دفعت وسائل التكنولجيا الحديثة بعض الجناة إلى محاولة استغلال التقدم العلمى فى نشر العديد من الصور الجنسية الفاضحة والافعال الفاحشة المخلة بالآداب العامة على شبكة الانترنت، والتى غالبا ما يكون محلا لها الاطفال الصغار سواء كان ذلك عن طريق تصويرهم فى اوضاع جنسية مخلة، أو استخدام التقنية الرقمية الحديثة (DIGITAL) فى تركيب صور اطفال ابرياء على اجساد عارية أو اوضاع جنسية بصورة تتعارض مع الاحترام الواجب لطفولتهم، كما اتخذ الاعتداء على الحق فى الصورة شكل الاعتداء على ملكية الشخص لصورته والاستغلال المالى لها.

أولا:جرائم اشاعة الصور والافعال الفاحشة المخلة بالآداب العامة على شبكة الانترنت

الاشاعة فى اللغة تعنى" أن الخبر ينتشر غير متثبت منه" وهى مشتقة من الفعل (اشاع) اى " أظهر ونشر"[١٠٦].

وتتحقق تلك الجرائم من خلال العديد من الافعال المادية التى تتجسد فى عرض أو نشر أو توزيع اية صور أو اقوال أو افعال فاحشة وفاضحة ومخلة بالآداب العامة على شبكة الانترنت ، كما تتحقق ايضا من خلال انشاء العديد من المواقع الجنسية على شبكة الانترنت والترويج لها أو استقطاب الزائرين اليها ، أو تبادل رسائل البريد الالكترونى التى تحوى العديد من الصور والاشارات والاقوال والافعال الفاحشة بين المستخدمين لشبكة الانترنت ، أو ارسال الرسائل

[١٠٦]- المعجم الوجيز ، مجمع اللغة العربية، الهيئة العامة لشئون المطابع الاميرية ، ١٩٩٠، ص ٣٥٧.

الجنسية عبر خدمة الرسائل فى البريد الالكترونى على شبكة الانترنت من مواقع جنسية مجهولة المصدر أو الهوية إلى العديد من المواقع على تلك الشبكة.

وقد يكون الغرض من تلك الجرائم ارتكاب العديد من افعال النصب والاحتيال المعلوماتى وقد يكون الغرض منها ايضا – وكما سبق أن بينا- اتلاف العديد من المكونات المنطقية للحاسب الآلى عن طريق استخدام الفيروسات الجنسية التى تقوم بعمليات التدمير لتلك المكونات.

ثانيا: جرائم الاستغلال الجنسى للاطفال عبر شبكة الانترنت:

" نتيجة للتقدم التكنولوجى الهائل فى مجال استخدام الحاسب الالى الإنترنت ، فقد ظهرت على الإنترنت بعض المواقع التى تتناول بالعرض والتوزيع صور خارجة للاطفال، مما دفع المجتمع الدولى إلى محاولة التدخل لوقف مثل تلك النشاطات والاعتداءات الاجرامية التى تمس الكرامة الانسانية والحياء العام، ولذا فقد لقى هذا الموضوع من قبل خبراء اليونسكو بباريس فى الفترة من ١٨-١٩ يناير ١٩٩٩، وكذلك ، فقد عقد المؤتمر الدولى لمكافحة استغلال الاطفال فى الجنس على الإنترنت فى الفترة من ٢٩ سبتمبر إلى الاول من اكتوبر ١٩٩٩ بڤيينا بالنمسا بمبادرة من وزير خارجية النمسا ووزيرة خارجية الولايات المتحدة الامريكية فى تلك الفترة، وقد اكد المؤتمر على تدعيم التعاون الدولى فى مجال مكافحة هذا النوع من النشاط، وتشجيع وضع قواعد ذاتية للسلوك من قبل موردى خدمة الإنترنت، وتشجيع انشاء خطوط ساخنة للاتصال تسمح للمواطنين بالابلاغ عن المواقع الاباحية للاطفال على الإنترنت ، وقد كان الهدف الرئيسى لذلك المؤتمر هو توعية الجمهور لمواجهة الاستغلال الجنسى للاطفال على الإنترنت، وخصوصا أن الإنترنت اصبح بالفعل جزءا من حياتنا اليومية سواء تعلق الامر بالاتصالات أو العمل أو التجارة، ومع الاخذ فى الاعتبار حق كل منا فى الاتصال بطريق الإنترنت ، وقد اكد هذا المؤتمر على انه فى اطار الحماية الخاصة للطفل بمقتضى الاتفاقية الدولية المتعلقة بحقوقه، فانه يقع التزام على عاتق الدول المختلفة بمحاربة الاستغلال التجارى للاطفال عن طريق الجنس،وقد اعترف المؤتمرون بتزايد مشكلة الاستغلال الجنسى للاطفال على الإنترنت، كما اكد المؤتمر على وجوب عدم التسامح مع مثل هذا الامر، وضرورة تدخل المشرع الوطنى لتجريم التجارة الجنسية على الإنترنت التى تنطوى على استغلال للطفولة، وتدعيم التعاون الدولى فى مجال مكافحة هذه الجرائم، وانشاء وحدات

خاصة لمكافحة هذه الجرائم، واعداد برنامج تدريب خاص للتاهيل فى هذا المجال، واكد المؤتمر كذلك على أنه يتعين على الدول المختلفة أن تضع قواعد دنيا يتم بمقتضاها وضع تعريف متقارب لهذه الجريمة واعتبار أن الحيازة العمدية وانتاج وتوزيع واستيراد وتصدير ونقل والاعلان عن صور الاطفال الاباحية بطريق الكمبيوتر أو وسائل التخزين الالكترونى من الجرائم المعاقب عليها، وانه يتعين من الناحية الاجرائية اتخاذ الإجراءات الكفيلة للمحافظة على البيانات المتحفظ عليها بما فيها تلك البيانات الموجودة تحت يد مورد خدمة الإنترنت ولو كان فى بلدآخر مع الاخذ فى الاعتبار المشكلات الخاصة بالتخزين وحجمه والاوامر القضائية ومقتضيات حماية البيانات والتى يمكن أن تكون محلا للمطالبة بتعاون متبادل بشان كل تفتيش أو قبض أو افشاء لمحتوى هذه البيانات، واوصى المؤتمر بضرورة اتخاذ اجراءات مشتركة تسمح بتجاوز الحدود لتفتيش وضبط اجهزة الكمبيوتر بما يسرع بالاجراءات الجنائية، علاوة على انه يتعين اقامة وسائل الاتصال الدائم لتحقيق التعاون الدولى فى هذا المجال.

المطلب التاسع
غسيل الأموال عبر الإنترنت

اولا: المقصود بغسيل الأموال:

يعني مصطلح غسيل الأموال أن هذه الأموال "القذرة إذا بقيت في أيدي حائزيها فإن ذلك يؤدي إلى اكتشاف نشاطهم الإجرامي وبالتالي فإن غسيل الأموال هي محاولة من هؤلاء الأشخاص المجرمين بكافة الطرق لإخفاء الأصل غير الشرعى لهذه الأموال لكى يوجه إلى الإستثمار فى أعمال اقتصادية كل البعد عن الأعمال غير الشرعية التي حصلت منها هذه الأموال[١٠٧].

وبعبارة اخرى اكثر تفصيلا، فان غسيل الأموال غير المشروعة أو الأموال القذرة هو جريمة من الجرائم الاقتصادية، تحكمها فى اغلب الاحوال قواعد القانون الجنائى الدولى، تتضمن عملية أو سلسلة من العمليات الاقتصادية والمالية المركبة، يبغى مرتكبها اضفاء الصفة الشرعية على اموال متحصلة من انشطة اجرامية ومصادر غير شرعية عن طريق اخفاء المصدر الاجرامى لهذه

[١٠٧]-أنظر : د/ عبد الرحمن صبرى ، غسيل الاموال فى اسواق المال الناشئة، مقالة منشورة بجريدة الاهرام، السنه ١٢٤، العدد رقم ٤١٢٥٨ بتاريخ ١٩٩٩/١١/٢٢ صفحة قضايا واراء.

الأموال، بما يمكن الجناة فى نهاية الامر من الانتفاع بتلك الأموال- فى طمأنينة ويسر- وادخالها فى دائرة التعامل الاقتصادى والمالى القانونى[١٠٨].

وجريمة غسيل الأموال- وكاية ظاهرة اجرامية- يلتزم لحققها وقيامها قانونا توافر اركان وعناصر معينة حيث لا تقوم تلك الجريمة بغير تحقق هذه الاركان وعناصرها مجتمعة ومكتملة، ويائتلف الركن المادى لتلك الجريمة من ثلاثة عناصر هى: وجود جريمة اولية أو اصلة سابقة تعتبر مصدرا للمال القذر غير الشروع، وان يتمخض عن تلك الجريمة مال غير نظيف، وان يقوم الجانى بارتكاب نشاط اجرامى يتحقق به غسل هذا المال عبر النظيف، ويتمثل هذا النشاط فى اجراء عملية أو سلسلة من العمليات الاقتصادية والمالية – البسيطة أو المركبة- بغية لتطهير تلك الأموال القذرة وادخالها إلى حيز الوجود المالى والاقتصادى والقانونى لتبدو فى النهاية كانها مشروعة من مصدر مشروع).

اما الركن المعنوى لجريمة غسيل الأموال فيحوى عنصرين هما: عنصر العلم (علم الجانى بعناصر الركن المادى لتلك الجريمة)، وعنصر الارادة (ارادة تحقيق النتيجة الاجرامية، التى تتمثل فى تلك الجريمة فى ارادة تطهير تلك الأموال واخفاء مصدرها الاجرامى غير المشروع).

ثانيأ: اساليب غسيل الأموال عبر شبكة الإنترنت:

لاشك أن التقدم العلمى الهائل فى مجال تكنولوجيا المعلومات ووسائل الاتصالات خاصة مع بداية النصف الثانى من القرن العشرين- كما سبق أن بينا- وشيوع استخدام تلك التكنولوجيا فى اجراء المعاملات المالية والائتمانية، قد امد الجناة فى جرائم غسيل الأموال ببدال وخيارات جسمية ومبتكرة وحديثة لارتكاب جرائمهم القذرة ومحو آثارها الاجرامية فى سهولة ويسر، ووضع فى ذات الوقت العديد من العراقيل والصعوبات والتحديات امام السلطات المختصة- من اجهزة ضبط ومكافحة وتحقيق وقضاء- بتعقب تلك الجرائم وملاحقة مرتكبيها وتقديمهم للعدالة وتنفيذ الجزاءات الجنائية عليهم.

ومن ثمرات هذا التقدم، والتى لاقت اهمية بالغة ودرسة تفصيلية فى

١٠٨-أنظر : د/ اشرف توفيق شمس الدين – دراسة نقدية القانون مكافحة غسل الأموال الجديد- دار النهضة العربية ٢٠٠٣ ص ٣.

الآونة الاخير لدى المتخصصين فى مجال الجريمة، وعلى وجه الخصوص" الجريمة المنظمة" ، استخدام مرتبكى جرائم غسل الأموال لشبكة الاتصالات الدولية عبر اجهزة الحاسب الآلى والمعروفة باسم (الإنترنت) للتحويل الالكترونى للاموال غير النظيفة من شخص لآخر- عن طريق اجهزة الحاسب الآلى الشخصية- عبر الدول، ودون حاجة إلى اللجوء لاساليب تحويل النقود والأموال التقليدية من خلال البنوك وغيرها من المؤسسات المصرفية .

وقد لوحظ أن الإنترنت يعد وسيلة مثالية لمرتبكى جرائم غسيل الأموال غير المشروعة، وخاصة وان بعض المجرمين يقوم بانشاء صندوق بريدية الكترونية باسماء وهمية، بل ويقوم البعض بتاسيس العديد من المراكز المالية- والمعروفة باسم" لاوفشور" – عن طريق شبكة الإنترنت ، وبالتالى فان كافة العمليات المالية التى يجرونها تكون- غالبا- باسماء وهمية أو خيالية، وبالاضافة إلى ذلك. فان هناك بنوكا عبر الإنترنت- مثل : (بنك الاتحاد الاوربى) " وهو اول بنك يتم تاسيسة على الإنترنت عام ١٩٩٤"- تمارس انشطتها عادة فى الدول أو الجزر التى تتبنى مبدا " سرية الحسابات البنكية" بصفة مطلقة، وتوفر تسهيلات كبيرة لجذب رؤوس الأموال اليها، ويمكن لعملاء هذه البنوك تحويل اموالهم بسهولة وسرعة فى سرية تامة، فيستطيع الشخص من منزلة- على سبيل المثال– عن طريق الكمبيوتر الشخصى المربوط بشكة الإنترنت أن يجرى العديد من العمليات المالية التى يريدها وهو يتمتع بدرجة عالية من السرية والحماية ، وتعرض بنوك الإنترنت هذه خدمات متعددة على الجمهور، منها: (فتح حساب مباشرة- سواء بالنسبة للافراد أو الشركات – مع امكان فتح حسابات بنكية رقيمة أو مشفرة ، وتحويل الأموال إلكترونيا فى اى مكان فى العالم وبجميع العملات، وارسال الشيكات لاى مستفيد فى اى بلد،والدفع المباشر عبر الإنترنت، وشراء وبيع جميع العملات إلى غير ذلك من الخدمات الائتمانية والبنكية الاخرى التى تقدمها تلك البنوك للعديد من عملائها والمستفيدين من خدماتها المتعددة)، ولاشك فى اهمية هذه البنوك بالنسبة للعديد من الجناة مرتكبى جرائم غسيل الأموال ، وتسهيلها الدائم للعديد من عمليات غسيل الأموال المنظمة التى تتم على اقليم اكثر من دولة، وقد أشارت بعض التقديرات إلى أن حوالى ٢٨.٥ مليار دولار امريكى يتم غسلها سنويا عبر الإنترنت لتخترق حدود ٦٧ دولة.

ومن اجل رصد عمليات وحجم واساليب غسيل الأموال فقد قامت الدول الصناعية السبع الكبرى اثناء قمه L'Arche التى عقدت فى باريس فى يوليو سنه ١٩٨٩، بانشاء مجموعة عمل مالى دولية اطلق عليها " فريق عمل المهام المالية FATF أو GAFI" لدراسة الوسائل اللازمة لمنع استخدام الانظمة البنكية الدولية فى غسل الأموال، ودراسة ومناقشة وسائل واتجاهات واساليب غسيل الأموال سنويا، وقد انضمت إلى تلك المجموعة المالية العديد من دول العالم، وقامت تلك الدول بارسال العديد من الخبراء الاقتصاديين والماليين لحضور اجتماعات تلك المجموعة التى تنعقد بصفة دورية كل سنة لمناقشة ودراسة المسائل السابق بيانها، بالاضافة إلى دراسة الاساليب الفعالة لمكافحة غسيل الأموال.

وقد قام فريق عمل المهام الدولية (FATF) برصد اهم اساليب غسيل الأموال عبر الإنترنت فى تقريرين متتاليين عن سنتين متتاليتين (التقرير الحادى عشر فى ٣ فبراير ٢٠٠٠ عن الفترة من (١٩٩٩- ٢٠٠٠) " (التقرير الثانى عشر فى ١ فبراير ٢٠٠١ عن الفترة من (٢٠٠٠- ٢٠٠١)"

وسنعرض فيما يلى لاهم ما جاء فى هذين التقريرين من اساليب لغسل الأموال عبر شبكة الإنترنت:

١- العمليات المصرفية عبر الإنترنت:

تقدم الاعداد المتزايدة من المؤسسات المالية فى الوقت الراهن خدمات مصرفية جزئية عبر الإنترنت، وفى الوقت ذاته، فان جهات اخرى تستخدم الإنترنت لتقديم خدمات غسل الأموال ، وفى بعض الاحيان يطلق على هذه الخدمات اسم " خدمات مالية مقدمة عن بعد " أو " فرص استثمارية" لاضفاء صبغة قانونية عليها، وفى ظل انتشار كل انواع النشاط التجارى عبر الإنترنت والامكانيات المرتقبة لاختراق هذه الوسيلة، قام خبراء FATF بدراسة هذا الموضوع بصورة دقيقة فى محاولة لالقاء المزيد من الاهتمام على الاحتمالات المرتقبة لاستخدام هذه الوسيلة (الإنترنت) فى عمليات غسيل الأموال ، ويأتى هذا الموضوع فى اطار مجهودات FATF الرامية إلى تحديد التضمينات الرئيسية لغسل الأموال الناتجة عن تقديم وسائل التكنولوجيا الحديثة.

وتختلف خدمات المعاملات التجارية من مؤسسات إلى اخرى عبر الإنترنت، ولكنها تتضمن العديد من الانشطة مثل : (فتح الحسابات الجديدة " كالشيكات والادخار ..وغيرها) ودفع الفواتير، والكروت الدائنة والمدينة، وكروت السحب من ماكينات الصرف الآلى، والاقراص عبر الإنترنت ، ومنح الودائع فى بعض الاحيان وعلى الرغم من تقديم بعض الخدمات عبر الإنترنت عن طريق بنوك تقتصر خدماتها على تلك المقدمة عبر الإنترنت ، فان المؤسسات التى تقدم خدمات المعاملات التجارية قائمة بالفعل، بالاضافة إلى المؤسسات التقليدية والتى تحولت إلى انظمة مصرفية عبر الإنترنت لتقديم خدمات اضافية لعملائها.

ويرتكز الاهتمام الرئيسى فيما يتعلق بالمعاملات المصرفية عن طريق الإنترنت فى الخفض الواضح للاتصالات المباشرة بين العميل والمؤسسة المالية، حيث يستطيع العميل الدخول إلى الحساب الخاص به عن طريق الكمبيوتر الشخصى باستخدام برامج استعراض الإنترنت، والدخول إلى الإنترنت على المستوى العالمى من خلال شركات توفير خدمات الإنترنت، ويتم الدخول فور قيام العميل بتقديم الكود الشخصى الخاص به إلى شبكة الإنترنت الخاصة بالبنك، ونظرا لان هذا الدخول غير مباشر، فان المؤسسة المالية لا يوجد لديها اى وسيلة للتاكد من هوية العميل الذى قام بالفعل بالدخول إلى الحاسب الآلى والوصول إلى الحساب المقصود، وبالاضافة إلى ذلك، فانه فى ظل السرعة المتزايدة للدخول على الإنترنت ، فان العميل يتمتع بامكانية الدخول إلى الحساب الخاص به من اى مكان فى العالم، ولا تتمكن المؤسسة من اثبات الموقع الذى تم منه الدخول إلى الحساب ، ويرجع ذلك إلى أن الدخول يتم عبر شركات توفير خدمات الإنترنت ، ومن ثم يتمكن اى فرد يرغب فى اخفاء هويته الحقيقية- من القائمين بعمليات غسيل الأموال أو اية انشطة اجرامية اخرى- من الحصول على حساب مصرفى على الإنترنت غير خاضع لاى ضوابط، كما يمكنه السيطرةعلى هذا الحساب من اى مكان فى العالم.

٢- انظمة التحويلات البديلة:

على الرغم من عدم وجود تعريف اصطلاحى متفق عليه على نطاق واسع فيما يتعلق بـ" انظمة التحويلات البديلة" ، فان هناك اتفاق جزئى حول الخصائص الشائعة لهذه المنظمة، وبادئ ذى بدء فانه ينبغى التنوية إلى أن نظام التحويلات البديلة يتم استخدامه للاشارة إلى ما يطلق عليه حاليا فى بعض

الاحيان اسم " انظمة سرية" أو " انظمة مصرفية موازية "وقد تطورت هذه الانظمة بوجه عام . اعتمادا على عوامل اخلاقية أو ثقافية أو تاريخية خاصة وفى بعض الحالات، شكلت هذه الانظمة الوسائل التقليدية لنقل الأموال وذلك قبل انتشار الانظمة المصرفية الغربية فى القرن التاسع عشر والقرن العشرين، ويتمثل العامل الرئيسى فى هذه الانظمة- والذى تشترك فيه مع النظام المصرفى الرسمى أو " البنك المراسل" فى نقل القيمة من مكان إلى آخر بدون الانتقال المادى للعملة، وتعمل انظمة التحويلات البديلة فى اغلب الاحيان- خارج الانظمة التشريعية المالية القومية، وهناك انظمة توظف عوامل من الاقتصاد القانونى أو حتى الخدمات المالية المنتظمة، الامر الذى يؤدى بدورة إلى صعوبة الكشف عن هذه الحالات من قبل سلطات تنفيذ القانون.

ويتمثل العامل الاساسى فى كل نظام من انظمة التحويلات البديلة فى أن كل هذه الانظمة تعتمد بصورة أو باخرى على اجراء "صافى القيمة" أو " التحويل الدفترى أو الاسمى" لنقل القيمة، وفى واقع الامر ، يتم استخدام هذه الانظمة فى اغلب الاحيان لتقديم خدمة مالية اساسية لبعض الجاليات المهاجرة، وتعد هذه الانظمة مضمونة إلى حد كبير، فضلا عن انها اقل تكلفة مقارنة بالبنوك التقليدية، اضف إلى ذلك انه يتم استخدامها فى بعض الاحيان للتهرب من صرف العملة الصارمة، وتقدم هذه الانظمة ايضا درجة من عدم المعرفة باسم المستخدم ، وهذه الخاصية الاخيرة – تقديم درجة من عدم المعرفة باسم المستخدم- دفعت البعض إلى استغلال هذه الانظمة فى اعمال غير مشروعة مدنيا وجنائيا.

وقد تناول الخبراء بالمناقشة – فى تقرير فريق عمل المهام المالية حول غسيل الأموال الصادر فى ٣ فبراير ٢٠٠٠ – نماذج رئيسية ثلاثة من انظمة التحويلات البديلة قد تستخدم فى غسل الأموال التى يكون الإنترنت احد وسائلها ، وهذه النماذج هى : (السوق السوداء لصرف عملة البيزو "BMPE" ، ونظام الحوالات المصرفية، والانظمة الصينية/ الشرق اوسطية"[١٠٩].

٣- استخدام الجهاز المصرفى (اون لاين) فى غسل الأموال:

تزايدت اعداد المؤسسات المالية التى تقدم الخدمات المصرفية أون لاين عبر شبكة الإنترنت فى الوقت الحاضر بصورة مذهلة، واثناء إجراء التدريبات

[١٠٩]- ملخص تقرير فريق عمل المهام المالية حول غسل الأموال (FATF) الحادى عشر (١٩٩٩-٢٠٠٠) ٣ فبراير ٢٠٠٠.

الرمزية للتقرير الثانى عشر لفريق عمل المهام المالية لغسيل الأموال (FATF) والصادر فى ١ فبراير ٢٠٠١ ، كثرت المناقشات حول العمليات المصرفية أون لاين، مما قد اثار العديد من الاهتمامات التى تداولت اثناء التدريب فى عام ٢٠٠٠، وعلى ذلك، فقد قيل أن الصفقات المالية التى تتم من خلال الإنترنت لا تشكل اى خطر على عملية غسل الأموال،ومع ذلك ، فان هناك ثلاث سمات خاصة للانترنت قد تساهم من جانبها فى اثارة عدد من المخاطر التقليدية لغسل الأموال، منها:

أ- تسهيل الاتصال من خلال الإنترنت
ب- تبدد صفة التواصل بين العميل والمؤسسة
ج- الاسراع فى اجراء الصفقة الإلكترونية.

وبعيدا عن الخلافات والمناقشات التى دارت فى الاجتماع الحادى عشر والثانى عشر لمجموعة العمل المالى الدولية (FATF) حول مدى توافر أو عدم توافر عميات غسل الأموال عن طريق استخدام الخدمات المصرفية اون لاين عبر شبكة الإنترنت، فقد استطاعت بعض الهيئات التشريعية – اثناء الاجتماع الثانى عشر لفريق عمل المهام المالية لغسل الأموال (FATF) - عرض عدد من القضايا التى من خلالها اصبح غسل الأموال مطبقا اعتمادا على نفس الوسائل المستخدمة فى قضايا الاحتيال الاخرى، ويستفيد مرتكبى تلك القضايا من نوعية التواصل من خلال الإنترنت، ولعل من اهم الطرق المستخدمة فى غسل الأموال عن طريق شبكة الإنترنت انشاء شركة للدفع عبر هذه الشبكة، وعلى ذلك فان القائم بعلميات غسل الأموال يعتمد على تلك الخدمات ، ويقوم بالسداد عن طريق استخدام كروت الائتمان أو الاقتراض بضمان الحسابات وخاصة فى مناطق الجريمة المتصلة ، وتقوم الشركة التابعة للقائم بعمليات غسل الأموال باعداد فاتورة لشركات كروت الائتمان والتى من جانبها تقوم بسداد قيمة الخدمات التى حصلت عليها، والشركة من ناحية اخرى تجد مبررا تلك المدفوعات، ومن خلال هذا النموذج يتضح أن القائم بغسل الأموال يتحكم فى الأموال المدفوعة والشركة التى تقدم الخدمة عبر الإنترنت، اما عن شركات كروت الائتمان وشركات الإنترنت وسداد الفواتير، والبنك الذى يبدا فى تنفيذ الاجراءات اللاشرعية، فان كلا منهم يعد مسئولا عن جزء من تلك العملية (عملية غسل الأموال غير المشروع) وفى واقع الامر، فان تلك العملية تتشابة مع عمليات الاحتيال مع

وجود بعض الاختلافات، حيث انه فى عملية الاحتيال نجد أن حسابات البنوك تنتمى لطرف ثالث برئ بدلا عن منفذ العملية.

ولعل من اهم المشاكل التى قد تواجه المحقق عند التطرق لتلك العملية هى صعوبة ادراك التواصل بين افراد العملية، حيث أن القائم بغسل الأموال يقوم من جانبة بالاعتماد على بعض المتطابقات الخرافية أو الخيالية وذلك لتسجيل وجودة على الشبكة، وعند التاكد من الاستفادة القصوى التى تعود عليه من الاتصال السهل والمباشر بشبكات الإنترنت فى مناطق جغرافية عدة،- ومن ثم التاكد من ابتعاده التام عن نشاطاته الاجرامية التى يقوم بها- سيكون على دراية وعلم بتفاوت التشابة فى اهم تسجيلات التواصل عبر شبكات الإنترنت التى يوفرها مقدمو الخدمة، وهذا بدوره سيجعل تسمية المحقق للعملية صعب للغاية، هذا بالاضافة إلى أن مكونات العملية ستكون مجزأة مما سيجعل الامر صعبا لتحديد ما إذا كان النشاط غير المشروع ذو اساس فعلى ام لا بغض النظر عن الادراك الكلى للعملية.

خلاصة القول، فان المجرم الذى يعتمد على شبكة الإنترنت يستفيد من بعض عناصر هذا النظام، مما يؤكد غموض الامر امام المحققين.

٤- المقامرة عبر شبكة الإنترنت :

تعد المقامرة عبر شبكة الإنترنت بمثابة خدمة جيدة للتستر على عمليات غسيل الأموال التى تتم عبر هذه الشبكة، وهناك ادلة ضمن تشريعات فريق عمل المهام المالية لغسيل الأموال (FATF) يتضح من خلالها أن المجرمين يعتمدون كليا على المقامرة عبر الإنترنت من اجل ارتكاب جرائم اخرى وغسل الأموال الناجمة عن ارتكاب تلك الجرائم.

وبالرغم من المحاولات المتعددة للتعامل مع جرائم المقامرة عبر شبكة الإنترنت- سواء عن طريق التحكم أو منح التراخيص أو الحظر الكلى- فقد تزايد ارتكاب تلك الجرائم بصورة كبيرة، فعلى سبيل المثال ، يتم اجراء الصفقات من خلال كروت الائتمان من ناحية، فى حين أن استبدال بعض مواقع المقامرة يجعل عمليات التشغيل والمتابعة للاطراف الاخرى وفريق عمل المهام المالية لغسيل الأموال (FATF) نحو تتبع تلك الجرائم اكثر صعوبة أن لم يكن مستحيلا، علاوة على ذلك فانه يتم رصد صفقات المقامرة لاهميتها وادارتها من خلال الإنترنت- حيث انها تعتمد اساس على البرمجة- ولكن هذا الأمر قد يواجه صعوبات فى جمع المعلومات والادلة

الخاتمة

كانت الغاية من هذه الدراسة، " جرائم الحاسب الآلى– دراسة تحليلية " إلقاء الضوء على هذا النوع من الجرائم .

وقد رأينا من خلال هذه الدراسة، كيف أصبحت الجريمة المعلوماتية بمختلف أبعادها وأشكالها جريمة العصر، حيث تعاظمت قوتها وخطورتها، لمواكبتها حركة التطور في شتى المجالات العلمية والتكنولوجية، واستطاعتها الاستفادة التامة من الثورة التكنولوجية في مجال الاتصالات والمواصلات.

لذا فهي أمر واقع فرض وجوده على رجال الفقه والقانون، لما يميزها من خصائص عن غيرها من الجرائم موضوع القانون الجنائي والقوانين الأخرى، وأصبحت من الموضوعات الساخنة المتداولة في المحافل الدولية والمؤتمرات الإقليمية، للبحث عن الصيغة المثلى والأسلوب الفعال تجاه مواجهة هذا النوع من الجرائم، بالنظر لجسامة الأضرار والأخطار المترتبة عن تزايد حجم نشاطها وتغلغلها في كافة أرجاء المعمورة.

والواقع أن هذه الدراسة ليست من السهولة بمكان، حيث يمكن القول بأن

ثورة الإتصالات والمعلومات أفرزت وسائل جديدة للبشرية تجعل الحياة أفضل من ذى قبل ,إنما فتحت الباب غلى مصراعيه لظهور صور من السلوك المنحرف إجتماعيا لم يكن من الممكن وقوعها فى الماضى وتخرج عن دائرة التجريم والعقاب القائمة ولأن المشرع لم يتصور حدوثها أصلا .

فمن جهة أولى أتاحت نظم الكمبيوتر ظهور صور جديدة من الجرائم لم تكن موجودة فى الماضى , وذلك مثل سرقة المعلومات والأسرار المودعة فى قواعد المعلومات , ومن جهة ثانية أتاحت هذة النظم الفرصة لإرتكاب الجرائم التقليدية بطرق غير تقليدية كما فى جرائم الغش واتلاف وافساد المعلومات المخزنة فى قواعد المعلومات .

ويمكن القول أن ظاهرة الجريمة المعلوماتية اليوم، أصبحت محور اهتمام الكافة من دول ومنظمات بأنواعها، بل هى حديث الناس في المنازل والأماكن العامة، والجميع يرى الظاهرة من وجهة نظر مختلفة، وأزعم أننى من خلال هذة الدراسة قد حاولت إلقاء الضوء على هذه الظاهرة، كمحاولة جادة للتعرف على الجوانب العديدة والمتشعبة لهذا النوع من الجرائم , واحسب اننى حاولت من خلال استخدام المنهج التحليلى لهذة الجريمة التوصل إلى أمور قد

تساعدنا على إستجلاء الموقف بطريقة مناسبة تقود إلى الإدراك والإلمام بالجوانب المرتبطة بهذة الجريمة ،

نظرا لأن هذة الجريمة تتميز بعدة خصائص لعل أبرزها ما يلى :-

- لايتم فى الغالب الأعم الإبلاغ عن جرائم الإنترنت إما لعدم إكتشاف الضحية لها وإما خشيته من التشهير , لذا نجد أن معظم جرائم الإنترنت تم اكتشافها بالمصادفة ، بل وبعد وقت طويل من ارتكابها علاوة على أن الجرائم المكتشفة هى أقل بكثير من تلك التى لم تكتشف بعد ، فالفجوة بين عدد هذة الجرائم الحقيقى وما تم اكتشافه فجوة كبيرة .
- من الناحية النظرية يسهل ارتكاب الجريمة ذات الطابع التقنى كما أنه من السهل إخفاء معالم الجريمة وصعوبة تتبع مرتكبيها .
- هذا النوع من الإجرام لايترك أثرا له بعد ارتكابها علاوة على صعوبة الإحتفاظ الفنى بآثارها إن وجدت , فهذة الجرائم لا تترك أثرا فليست هناك اموال أو مجوهرات مفقودة إنماهى أرقام تتغير فى السجلات ولذا فإنة معظم جرائم الإنترنت تم اكتشافها بالمصادفة وبعد وقت طويل من ارتكابها
- تعتمد هذة الجرائم على قمة الذكاء فى ارتكابها ويصعب على المحقق التقليدى التعامل مع هذة الجرائم إذ يصعب عليه متابعة جرائم الإنترنت والكشف عنها واقامة الدليل عليها فهى جرائم تتسم بالغموض واثباتها من الصعوبة بمكان والتحقيق فيها يختلف عن التحقيق فى الجرائم التقليدية
- الوصول إلى الحقيقة بشأنها يستوجب الإستعانة بخبرة فنية عالية المستوى
- عولمة هذة الجرائم يؤدى إلى تشتيت جهود التحرى والتنسيق الدولى لتعقب مثل هذة الجرائم فهذة الجرائم هى صورة صادقة من صور العولمة فمن حيث المكان يمكن إرتكاب هذة الجرائم عن بعد , وقد يتعدد هذا المكان بين أكثر من دولة , ومن ا لناحية الزمنية تختلف المواقيت بين الدول , الأمر الذى يثير التساؤل حول تحديد القانون الواجب التطبيق على هذة الجريمة فئات الجناة فى هذا المجال تشمل فئات متباينة هى :-

أ- مستخدمو الحاسب بالمنازل

ب- الموظفون الساخطون على منظماتهم

ت- المتسللون ومنهم الهواة والعابثين بقصد التسلية

ث- المحترفون الذين يتسللون إلى مواقع مختارة بعناية ويعبثون أو يتلفون النظام أو يسرقون محتوياته , وتقع أغلب جرائم الإنترنت حاليا تحت هذة الفئة

ج- العاملون فى الجريمة المنظمة .

ومن الجدير بالذكر ان هذة الدراسة تمت على الوجه التالى :-

قامت الدراسة على ثلاثة فصول , وقد مهدت لها بتقديم عام حيث تضمن : أهمية دراسة جرائم الحاسب الآلى _ صعوبة الدراسة _ إختيار موضوع الدراسة _ منهج الدراسة _ خطة الدراسة .

وقد تناول الفصل الأول التأصيل التاريخى لتشريعات جرائم الكمبيوتر, وذلك من خلال تمهيد ومبحثين , حيث خصصت المبحث الأول للتأصيل التاريخى لتشريعات جرائم الحاسب الآلى ثم خصصت المبحث الثانى لمفهوم قانون الكمبيوتر , و من خلال المبحث الاول يتبين لنا ان محاولة تقصي التدابير التشريعية في مجال تقنية المعلومات يعني العودة الي السبعينات,فالتطور التاريخي لتقنية المعلومات يشير الي ان السبعينات تحديدا شهدت انتقالا حقيقيا في ميدان الحوسبة ,وتقاربها بانظمة الاتصالات .

و من خلال هذا المبحث ايضا توصلت الي ثلاث حقائق الاولي ان بداية قانون الكمبيوتر ارتبط بالبحث في المسئولية عن انشطة تتصل بالمعلومات ونظمها و تحديدا في المجال الجزائي.

و الثانية ان الخصوصية و حماية البيانات تمثل اول مجال من مجالات قانون الكمبيوتر من حيث الاهتمام الدولي .

و الحقيقة الثالثة ان اكثر تشريعات قانون الكمبيوتر نضجا ووضوحا في اغراضها القوانين او التدابير التشريعية المتعلقة بحماية الملكية الفكرية لبرامج الكمبيوتر و يتصور ان تحقق هذة التشريعات حماية اوسع في السنوات القادمة في مجال اسماء مواقع الانترنت والمحتوى الرقمي لمواقع الانترنت.

و من خلال المبحث الثاني(مفهوم قانون الكمبيوتر)راينا ان المجالات التشريعية في هذا المجال تؤدي إلى تبلور قانون الكمبيوتر كافرع مستقلة عن بقية الفروع القانونية وقد تطرقنا من خلال هذا المبحث الي ان اساس قانون الكمبيوتر و مبرر وجوده الحماية القانونية للمعلومات فان قصرة علي جرائم الكمبيوتر المتصلة بحماية استخدام الكمبيوتر و مخزونه المعلوماتي و الحق في ملكية المعلومة ذات القيمة الاقتصادية اما بذاتها او بما تمثلة قد اغفل حماية اخري و انماطا معلوماتية اخري فاغفل بذلك البيانات الشخصية مثلا واغفل

حماية انماط التعامل الالكتروني مع المعلومات و اغفل العلاقات العقدية في بيئة المعلومات و قصره ايضا علي حماية الملكية الفكرية يحقق الحماية فقط لاوعية المعلومات و اشكالها النهائية المنطوية
علي عنصر ابداعي و يغفل حماية استخدام نظمها و يغفل حماية المعلومات ذات القيمة الاقتصادية و مثل هذا القول ينسحب علي اي رأي يحصر قانون الكمبيوتر بأحد مجالاته ليكون عاجزا عن شمول مفردات حماية المعلومات .

وبالفصل الثانى مدلول الجريمة المعلوماتية حيث ذهبنا إلى أن تعريف الجريمة المعلوماتية هو كل نشاط إجرامى يؤدى فيه نظام الحاسب الآلى دورا لإتمامه على أن يكون هذا الدور على قدر من الأهمية .

وقد تناولنا هذا الفصل من خلال مبحثين خصصنا الأول لماهية المعلومات والثانى خصائص الجريمة المعلوماتية .

والفصل الثالث تقسيم جرائم المعلوماتية , حيث تناولت هذا الفصل من خلال مبحثين , خصصت الأول للجرائم التى تقع على الحاسب الآلى ومكوناته وخصصت الثانى للجرائم التى ترتكب بواسطة الحاسب الآلى ومكوناته .

وقد تناولت المبحث الأول من خلال ست مطالب على النحو التالى:

المطلب الأول: سرقة البرامج والمعلومات المخزنة آلياً.

المطلب الثانى: سرقة منفعة الحاسب الآلى أو الاستعمال غير المصرح به لنظام الحاسب الآلى.

المطلب الثالث: بعض أفعال تزوير المعلومات والبيانات والبرامج المخزنة آلياً والتلاعب بها.

المطلب الرابع: إختراق الحاسب الآلى وإنتحال هوية المستخدم.

المطلب الخامس: التجسس المعلوماتى

المطلب السادس: الإتلاف المعلوماتى

أما المبحث الثانى فقد تناولته من خلال تسع مطالب على النحو التالى:-

المطلب الأول : الاحتيال المعلوماتى

المطلب الثانى : التزوير المعلوماتى

المطلب الثالث : النصب المعلوماتى

المطلب الرابع : جرائم الاعتداء على حرية الحياة الخاصة

المطلب الخامس : جرائم الاعتداء على حقوق الملكية الفكرية والادبية.
المطلب السادس : جرائم إفشاء الاسرار فى اطار المعلوماتية
المطلب السابع : جرائم السب والقذف عبر الإنترنت.
المطلب الثامن : الجرائم المخلة بالآداب العامة فى اطار المعلوماتية
المطلب التاسع : غسيل الأموال عبر الإنترنت

وبما تقدم أكون قد فرغت من دراستى هذة وأحسب أننى لا أدعى بأن هذة الرسالة قد تناولت الموضوع من كل جوانبه نظرا لأن ذلك ليس بالعمل اليسير ولكن كل ما أتمناه أن أكون قد أضفت بهذة الدراسة ولو نقطة واحدة تظل مضيئة على مر التاريخ ومن خلال هذا البحث أزعم أن هناك بعض النتائج قد وضحت لنا ومنها حددنا بعض التوصيات ربما الأخذ بها قد يساهم فى سد نقص أو علاج ثغرة :

<u>اولا : النتائج :-</u>

١- مبدأ الشرعية الجنائية يفرض عدم جواز التجريم و العقاب عند إنتفاء النص , الأمر الذى يمنع مجازاة مرتكبى السلوك الضار أو الخطر على المجتمع بواسطة الكمبيوتر طالما أن المشرع الجنائى لم يقم بسن التشريعات اللازمة لإدخال هذا السلوك ضمن دائرة التجريم والعقاب وبالتالى على المشرعين مواكبة التطورات وسن التشريعات اللازمة للتصدى لظاهرة الإجرام المعلوماتى .

٢- انعدام وجود تصور واضح المعالم للقانون والقضاء تجاه جرائم الإنترنت لكونها من الجرائم الحديثة , وتلك مشكلة أكثر من كونها ظاهرة ولانعدام وجود تقاليد بشأنها كما هو الشأن فى الجرائم الأخرى ويساعد ذلك إنعدام وجود مركزية وملكية عبر الإنترنت .

٣- رغم صدور عدد من التشريعات العربية بشأن حماية الملكية الفكرية والصناعية التى تضمنت النص على برامج الحاسب واعتبرتها من ضمن المصنفات المحمية فى القانون إلا أنه مكافحة الجرائم المعلوماتية فى الدول العربية مازالت بلا غطاء تشريعى يحددها ويجرم كافة صورها , وإذا كان التشريعات العربية بصفة عامة قاصرة فى مجال ملاحقة صور السلوك الضاروالخطر المتعلقة باستخدام الحاسوب (الكمبيوتر)

والإنترنت , فإن هذا القصور إنعكس مردوده على الجانب الإجرائى المتعلق بمكافحة الإجرام المعلوماتى , فلم تصدر تشريعات جنائية إجرائية كافية لتعقب مقترفى هذا الإجرام .

٤- تتعدد مظاهر القصور التشريعى التى يتعين أن تواجه كافة مظاهر السلوك السلبى المتعلقة بتقنية المعلومات , فالتشريعات مازالت ناقصة وقاصرة فى مجالات عدة منها على سبيل المثال :

- التشريعات الخاصة بالملكية الفكرية فيما يتعلق بأسماء مواقع الإنترنت وعناصرها ومحتواها والنشر الإلكترونى , وفى حقل التنظيم الصحفى للنشر الإلكترونى
- تنظيم التجارة الإلكترونية والتشريعات الضريبية التى تغطى الميادين الخاصة بالضريبة فى ميدان صناعة البرمجيات والأعمال على الإنترنت والتجارة الإلكترونية
- مقاييس إطلاق التقنية .
- القواعد التشريعية لنقل التكنولوجيا .
- التراخيص والإستثمار والضرائب المتعلقة بتكنولوجيا المعلومات .
- تنظيم حجية ومقبولية مستخرجات الحاسب .
- وسائل الإثبات التقنية والإثبات المدنى .
- تنظيم الصور الإجرامية فى ميدان الحاسب والإنترنت .
- أنظمة الدفع النقدى الإلكترونى .
- تنظيم عمل مقاهى الإنترنت .
- البرمجيات الصناعية .

٥- التفتيش على أجهزة الحاسوب : يجب أن تخضع لقواعد مختلفة عن القواعد العادية للتفتيش للبحث عن أداة الجريمة العادية ,ورغم ذلك نجد أن التشريعات العربية فى مجملها لم تحدد قواعد خاصة للتفتيش على الحاسبات الالية وكيفية وضبط المعلومات التى تحويها ومراقبة المعلومات أثناء إنتقالها, كما أن الإجراءات الجنائية للجهات القائمة على التفتيش غير حاسمة بشأن مسألة ضبط برامج الحاسب والمعلومات الموجودة بالأجهزة وفقا للشروط الخاصة بالإجراءات العادية للتفتيش .

٦- إذا كان المحقق مهمته البحث عن الحقيقة وإذا كان القاضى مهمته الفصل فيما يعرض عليه من منازعات , فعمل كلاهما يحتاج إلى بيئة قانونية تساعد على أداء الوظيفة , وهذة البيئة القانونية مازالت غامضة أو قاصرة ومواطن القصور والغموض متعددة منها :

- هل إعتداءات الأشخاص على الأموال فى البيئة الحقيقية يمكن تطبيق مفهومها على اعتداءات المجرم المعلوماتى ؟
- هل المعلومات بذاتها لها قيمة مالية ؟ ام هى تكون كذلك عندما تمثل أصولا أو حقوقا ؟
- كيف يمكن حماية السر التجارى أو الأسرار الشخصية وبيانات الحياة الخاصة من إعتداءات المجرم المعلوماتى أو المتطفل دون تصريح وإذن
- هل هناك معايير تحكم مقدمى خدمات الإنترنت بأنواعها ؟
- ما مدى المسئولية القانونية فى حالة تحميل الملفات الموسيقية من الإنترنت بغير موافقة صاحب الموقع ؟
- هل يعتبر النشر الإلكترونى من قبيل النشر الصحفى المنظم فى تشريعات الصحافة والمطبوعات ؟
- هل إبرام العقد بالإنترنت تتوافر فيه سلامة وصحة التعبير عن الإرادة بالقدر الذى يوفره التعاقد الكتابى او الشفهى فى مجلس العقد العادى ؟
- هل توقيع العقود والمراسلات إلكترونيا يتساوى مع توقيعها ورقيا ؟
- هل ما يعتد به من دفوع وإحتجاجات بشأن إلتزامات أطراف التعاقد أو علاقات الدفع التقليدية متاح بذاته أو أقل منه أو أكثر فى البيئة الرقمية؟
- هل لرسائل البريد الإلكترونى حجية فى الإثبات؟ وهل لها ذات قيمة المراسلات الورقية ؟
- هل الإنتخاب الإلكترونى هو تصويت صحيح ومقبول لمن إخترناه ممثلا لنا فى عالم المكان والجغرافيا ؟
- هل العلامة التجارية محمية من أن تكون إسم بطلق لطرف آخر ؟
- ماذا عن تصميم الموقع .. هل ثمة قدرة على منع الآخرين من سرقته واستخدامه ؟
- ماذا إن تم ربط موقعك على الإنترنت مع موقع لا ترغب فيه ان يكون بينهما رابط ؟

- ماذا عن فرض المحتوى على المستخدم .. هل يظل المستخدم عاجزا لاحول له ولاقوة أمام تدفق مواد لايرغبها أو لا يطلبها على صندوق بريده او خلال تصفحه المواقع التى يريدها ؟
- هل إغلاق المواقع ذات المحتوى غير المشروع فى بعض النظم والمشرع فى غيرها تجاوز على ديمقراطية العالم التخيلى ؟
- متى نشأ النزاع أيا كان وصفه أو مصدره فمن هو القاضى الرقمى ؟
- ما هو القانون الذى يحكم النزاع ؟ وما المحكمة ؟ وما المحكم ؟
- ما هى أخلاق المجتمع الرقمى وقواعد السلوك فيه .. هل ذاتها أخلا ق العالم الحقيقى أم ثمة تباين فى المفهوم والقيود ؟
- هل ثمة قدرة للمستخدم أن يطالب بحقوق فى مواجهة الطرف الوسيط فى كل تعامل أو إستخدام نتج عنه مساسا بحق من حقوقه ؟
- من هو حاكم الإنترنت .. وما الدستور الذى يحكمه ومن الشرطى الذى يهرع له المستخدم إذا تعرض لإعتداء سافر على حقوقه أو بياناته أو محتوى موقعه أو رسائله أو خصوصيته ؟
- كيفية حماية برامج الحاسب ؟
- كيفية مقاضاة مزورى خدمة الإنترنت على إنقطاع الخدمة ؟
- مراقبة أداء الموظفين عبر البريد الإلكترونى ورسائلهم فى بيئة العمل
- هل إرسال رسالة مازحة عبر البريد الإلكترونى يمكن أن تشكل جريمة جنائية وهل يمكن أن ترتب مسئولية مدنية ؟

كل ما سبق يعد من قبيل الفراغ التشريع فى مجال مكافحة الجرائم المعلوماتية ومما لاشك فيه أن هناك أسبابا تستوجب سد هذا الفراغ منها:-

١- سهولة إخفاء الجريمة : فالجريمة المعلوماتية غالبا مستترة وخفية
٢- نقص خبرة الشرطة وجهات الإدعاء والقضاء
٣- صعوبة الوصول إلى مرتكبى أغلب الجرائم المعلوماتية
٤- صعوبة الإثبات وذلك يرجع إلى الطبيعة الخاصة للدليل فى الجرائم المعلوماتية وصعوبة الوصول إليه وسهولة محوه وكذا أدلة الإدانة ذات نوعية مختلفة فهى معنوية الطبيعة
٥- إحجام الجهات والأشخاص المجنى عليهم عن الإبلاغ عن الجرائم المعلوماتية

٦- وجود العديد من الصعوبات الشديدة فى ضبط وتوصيف الجرائم المعلوماتية .

ثانيا التوصيات :-

بعد ان عرضنا النتائج المستخلصة من الدراسة فإننا نرى لزاما أن نعرض الحلول المقترحة على النحو التالى :-

١- ضرورة تقنين قواعد جديدة لمكافحة الجرائم المعلوماتية تؤخذ بعين الإعتبار للطبيعة الخاصة بهذة الجرائم ولا سيما فيما يتعلق بالإثبات فى الدعاوى الناشئة عن هذة الجرائم سواء فى ذلك الدعاوى الجنائية والمدنية والتأديبية , كما ينبغى تعديل قواعد الإجراءات الجنائية لتتلائم مع هذة الجرائم

٢- ضرورة التنسيق والتعاون الدولى قضائيا واجرائيا فى مجال مكافحة الجرائم المعلوماتية

٣- ضرورة تخصيص شرطة خاصة لمكافحة الجرائم المعلوماتية , وذلك من رجال الشرطة المدربين مع أجهزة الحاسوب والإنترنت

٤- يتعين تدريب رجال النيابة العامة والقضاء بشأن التعامل مع اجهزة الحاسوب والإنترنت

٥- ينبغى أن تنص التشريعات العربية على أن الإنترنت من وسائل العلانية فى قانون العقوبات والقوانين ذات الصلة بالجرائم المعلوماتية مع الأخذ فى الإعتبار أن الإنترنت اوسع إنتشارا من وسائل نشر أخرى

٦- يجب تعديل قانون إجراءات الجنائية لبيان مايجب إتباعه من أحكام حال التفتيش على الحاسبات وعند ضبط المعلومات التى تحتويها وضبط البريد الإلكترونى حتى يستمد الدليل مشروعيته

٧- ينبغى أن يسمح للسلطات القائمة بالضبط والتحقيق بضبط البريد الإلكترونى واية تقنية أخرى قد تفيد فى إثبات الجريمة والحصول على دليل والكشف عن الحقيقة

٨- ضرورة النص صراحة فى القوانين المنظمة للإثبات الجنائى والمدنى بما يسمح للقاضى بأن يستند إلى الأدلة المستخرجة من الحاسب الآلى والإنترنت , طالما أن ضبط هذة الأدلة جاء وليدة إجراءات مشروعة وتتم مناقشة هذة الأدلة بالمحكمة وبحضور خبير

٩- يجب إعتبار نشر وطباعة الصور الجنسية عن طريق الإنترنت مما يدخل ضمن زمرة جرائم الآداب

١٠- ضرورة تجريم استخدام الأطفال فى تصوير أفلام تمثلهم فى أوضاع مخلة بالآداب العامة وعرضها على شبكة الإنترنت

١١- ضرورة تجريم الدخول غير المصرح به على البريد الإلكترونى لإتلاف محتوياته

١٢- ضرورة نشر الوعى بين صفوف المواطنين وخاصة الشباب بخاطر التعامل مع المواقع السيئة على شبكة الإنترنت

١٣- ضرورة إدخال مادة أخلاقيات استخدام الإنترنت ضمن المناهج الدراسية فى التعليم قبل الجامعى

١٤- ضرورة إنشاء قسم بكليات الحقوق للجرائم المعلوماتية وتشجيع طلاب الدراسات العليا على الدراسة والبحث فيه

وبذا أكون قد فرغت من هذة الدراسة (جرائم الحاسب الآلى –دراسة تحليلية) ومنتهى املى وهدفى أن تكون قد حققت ماهو مستهدف منها وتكون إضافة حقيقية يمكن الإستفادة منها فى هذا المضمار .....

والله ولى التوفيق ...

المراجع

١- د/ احمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلى، دار النهضة العربية، ٢٠٠٠

٢- د/ اشرف توفيق شمس الدين – دراسة نقدية القانون مكافحة غسل الأموال الجديد- دار النهضة العربية ٢٠٠٣

٣- د/ سعيد عبد اللطيف حسن – إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت – (الجرائم الواقعة فى مجال تكنولوجيا المعلومات) – دار النهضة العربية- القاهرة- الطبعة الأولى – ١٩٩٩

٤- د / حسن صادق المرصفاوى، قانون العقوبات الخاص، منشاة المعارف، الاسكندرية، ١٩٩١

٥- د/ على عبد القادر القهوجى، د. فتوح عبد الله الشاذلى ، شرح قانون العقوبات " القسم الخاص" ، دار المطبوعات الجامعية، الاسكندرية، ١٩٩٩، الكتاب الثانى" جرائم الاعتداء على الانسان والمال

٦- عبد الرحمن صبرى ، غسيل الاموال فى اسواق المال الناشئة، مقالة منشورة بجريدة الاهرام، السنه ١٢٤، العدد رقم ٤١٢٥٨ بتاريخ ١٩٩٩/١١/٢٢ صفحة قضايا واراء.

٧- محمد أمين الرومى- جرائم الكمبيوتر والأنترنت –دار المطبوعات الجامعية الاسكندرية ٢٠٠٣

٨- د/ محمد شامى الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات ، ط٢ دار النهضة العربية، ١٩٩٨

٩- د/ محمد الامين البشرى- التحقيق فى جرائم الحاسب الآلى – بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت-كلية الشريعة والقانون-جامعة الإمارات مايو ٢٠٠٥

١٠- د /مدحت رمضان- جرائم الاعتداء على الاشخاص والانترنت – دار النهضة العربية – ٢٠٠٠

١١- د/ نائلة محمد فريد – جرائم الحاسب الإقتصادية (دراسة نظرية وتطبيقية) دار النهضة العربية- القاهرة ، ٢٠٠٤

١٢- د / نبيل على- الثقافة العربية وعصر المعلومات، منشورات دار المعرفة، العدد ٢٦٥ يناير ٢٠٠١

١٣- د/ هشام محمد فريد رستم- قانون العقوبات ومخاطر تقنية المعلومات مكتبة الآلات الحديثة- أسيوط ١٩٩٤

١٤- د/ هدى حامد قشقوش ، جرائم الحاسب الالكترونى فى التشريع المقارن، دار النهضة العربية، القاهرة، ١٩٩٢

المراجع عبر الإنترنت :-

Mark Grossaman
على الانترنت حيث يهتم بقانون الكمبيوتر منذ عام ١٩٩٦-
www.mgrossmanlaw.com
The cyberlaw encyclopedia. http://gahtan.com\techlaw
Lawoffc@nol.com.jo
Ulrich sieber (legal aspects of computer – related crimes, eu comcrime, 1998). الكتاب الخامس من موسوعة القانونية وتقنية المعلومات) دليل التجارة الدولية والاستثمار (اتفاقيات منظمة التجارة الدولية) عبر شبكة الإنترنتwww.law-d7.com

المراجع الأجنبية :-

- Barry B. Sookman, Sookman computer Law: Acquiring protecting Information Technology, Carwell Legal Pubns, April 2000.
- David Bainbridge- Introduction to computer Law, 5th edition, Finical Times Management, 2000.
- Emmanuel Michau, Computer Law in France, the computer law association, May 1998
- Ricardo Barretto & Ferreira da Silva, Computer Law in Latin America, The computer law Association, December, 1997.
- Vanessa Marsland, European Computer Law: An Introductory Guide, The computer law Association, December, 1996.
- Lawrence M Hertz, The computer and the law , Mathew

Bender & Company, 1999 USA.
- Peter B. Maggs, Computer Law: Cases, comments, and Questions. West wads worth, 1996.
- Computer Law Forms Hand book, Clark Boardman Callaghan, 1995.
- John Zeleznikow. Dan Hunter, Building Intelligent Legal Information systems, little Brown & company, 1994.
- Reba A. Best, D. Cheryn Picquet, Computer law and software protection., Mcfarland & company, 1993.
- G.P.V Vandenberghe, Advanced Topics, of law and Information technology, kluwer Law International. July 1989.
- A.W.Koers, Knowledge Based Systems in Law, Kluwer law International. July 1989.
- Richard L. Bernacchi, Aguide to the Legal and Management Aspects of Computer Thechnology, little Brown & Company, 1986, (2nd edition 1993).
- Colin Tapper, Computer Law, Longman 1982 (first edition 1978).
- Daniel Brooks, Computer Law, Parctising Law Inst. 1982.